# ENHANCED DIRECT ENROLLMENT AGREEMENT BETWEEN ENHANCED DIRECT ENROLLMENT ENTITY AND THE CENTERS FOR MEDICARE & MEDICAID SERVICES FOR THE INDIVIDUAL MARKET FEDERALLY-FACILITATED EXCHANGES AND STATE-BASED EXCHANGES ON THE FEDERAL PLATFORM

**THIS ENHANCED DIRECT ENROLLMENT AGREEMENT** ("Agreement") is entered into by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES ("CMS"), as the Party (as defined below) responsible for the management and oversight of the Federally-facilitated Exchanges ("FFEs"), also referred to as "Federally-facilitated Marketplaces" or "FFMs" and the operation of the federal eligibility and enrollment platform, which includes the CMS Data Services Hub ("Hub"), relied upon by certain State-based Exchanges (SBEs) for their eligibility and enrollment functions (including State-based Exchanges on the Federal Platform (SBE-FPs)), and _____
(hereinafter referred to as "Enhanced Direct Enrollment [EDE] Entity"), which uses a non-FFE Internet website in accordance with 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or 156.1230 to assist Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives in applying for Advance Payments of the Premium Tax Credit ("APTC") and Cost-sharing Reductions ("CSRs"); applying for enrollment in Qualified Health Plans ("QHPs"); completing enrollment in QHPs; and providing related Customer Service. CMS and EDE Entity are hereinafter referred to as the "Party" or, collectively, as the "Parties."

**WHEREAS:**

Section 1312(e) of the Affordable Care Act ("ACA") provides that the Secretary of the U.S. Department of Health & Human Services ("HHS") shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals in QHPs through an Exchange, and to assist individuals in applying for APTC and CSRs, to the extent allowed by States. To participate in the FFEs or SBE-FPs, Agents and Brokers, including Web-brokers, must complete all applicable registration and training requirements under 45 C.F.R. § 155.220.

Section 1301(a) of the ACA provides that QHPs are health plans that are certified by an Exchange and, among other things, comply with the regulations developed by the HHS under Section 1321(a) of the ACA and other requirements that an applicable Exchange may establish.

To facilitate the eligibility determination and enrollment processes, CMS will provide centralized and standardized business and technical services ("Hub Web Services") through application programming interfaces ("APIs") to EDE Entity that will enable EDE Entity to host application, enrollment, and post-enrollment services on EDE Entity's own website. The APIs will enable the secure transmission of key eligibility and enrollment information between CMS and EDE Entity.

To facilitate the operation of the FFEs and SBE-FPs, CMS desires to: (a) allow EDE Entity to create, collect, disclose, access, maintain, store, and use Personally Identifiable

Information ("PII") it receives directly from CMS and from Consumers, Applicants, Qualified Individuals, and Enrollees through EDE Entity's website—or from these individuals' legal representatives or Authorized Representatives—for the sole purpose of performing activities that are necessary to carry out functions that the ACA and its implementing regulations permit EDE Entity to perform; and (b) allow EDE Entity to provide such PII and other Consumer, Applicant, Qualified Individual, and Enrollee information to the FFEs and SBE-FPs through specific APIs to be provided by CMS.

EDE Entity desires to use an EDE Environment to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to perform the Authorized Functions described in Section III.a of this Agreement.

45 C.F.R. § 155.260(b) provides that an Exchange must, among other things, require as a condition of contract or agreement that Non-Exchange Entities comply with privacy and security standards that are consistent with the standards in 45 C.F.R. §§ 155.260(a)(1) through (a)(6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 C.F.R. § 155.260(a)(3). 45 C.F.R. § 155.280 requires HHS to oversee and monitor Non-Exchange Entities for compliance with Exchange-established privacy and security requirements.

CMS has adopted privacy and security standards with which EDE Entity must comply, as specified in the Non-Exchange Entity System Security and Privacy Plan ("NEE SSP")[1] and referenced in Appendix A ("Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities"), which are specifically incorporated herein. The security and privacy controls and implementation standards documented in the NEE SSP are established in accordance with Section 1411(g) of the ACA (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 ("FISMA") (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the standards in 45 C.F.R. §§ 155.260(a)(1) through (a)(6).

Now, therefore, in consideration of the promises and covenants herein contained, the adequacy of which the Parties acknowledge, the Parties agree as follows:

I. Definitions.

Capitalized terms not otherwise specifically defined herein shall have the meaning set forth in the attached Appendix B ("Definitions"). Any capitalized term that is not defined herein or in Appendix B has the meaning provided in 45 C.F.R. § 155.20.

[1] The NEE SSP template is located on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

II. Interconnection Security Agreement (ISA) Between Centers for Medicare & Medicaid Services (CMS) and Enhanced Direct Enrollment (EDE) Entity ("ISA").

If EDE Entity is a Primary EDE Entity, it must enter into an ISA with CMS. EDE Entity must comply with all terms of the ISA,[2] including the privacy and security compliance requirements set forth in the ISA. The ISA shall be in effect for the full duration of this Agreement. If an Upstream EDE Entity is using a Primary EDE Entity's EDE Environment, the Primary EDE Entity must supply an NEE SSP to each Upstream EDE Entity using the Primary EDE Entity's EDE Environment that identifies all Common Controls and Hybrid Controls implemented in the EDE Environment. All Common Controls and Hybrid Controls must be documented between each applicable Upstream EDE Entity and its Primary EDE Entity as required by the NEE SSP section "Common and Hybrid Controls." Furthermore, Appendix B of the ISA requires a Primary EDE Entity to attest that it has documented and shared the NEE SSP inheritable Common Controls and Hybrid Controls with applicable Upstream EDE Entities.

III. Acceptance of Standard Rules of Conduct.

EDE Entity and CMS are entering into this Agreement to satisfy the requirements under 45 C.F.R. §§ 155.260(b)(2) and 155.221(b)(4)(v). EDE Entity hereby acknowledges and agrees to accept and abide by the standard rules of conduct set forth below and in the Appendices, which are incorporated by reference in this Agreement, while and as engaging in any activity as EDE Entity for purposes of the ACA. EDE Entity shall strictly adhere to the privacy and security standards—and ensure that its employees, officers, directors, contractors, subcontractors, agents, Auditors, and representatives strictly adhere to the same—to gain and maintain access to the Hub Web Services and to create, collect, disclose, access, maintain, store, and use PII for the efficient operation of the FFEs and SBE-FPs. To the extent the privacy and security standards set forth in this Agreement are different than privacy and security standards applied to EDE Entity through any existing agreements with CMS, the more stringent privacy and security standards shall control.

a. Authorized Functions. EDE Entity may create, collect, disclose, access, maintain, store, and use PII for the following, if applicable:

    1. Assisting with completing applications for QHP eligibility;

    2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons;

    3. Assisting with completing applications for the receipt of APTC or CSRs and with selecting an APTC amount;

    4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR determination, if applicable;

    5. Assisting with the application for and determination of certificates of exemption;

[2] Unless specifically indicated otherwise, references to the ISA refer to the current, legally enforceable version of the agreement. The ISA is available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

6. Assisting with filing appeals of eligibility determinations in connection with the FFEs and SBE-FPs;

7. Transmitting information about the Consumer's, Applicant's, Qualified Individual's, or Enrollee's decisions regarding QHP enrollment and/or CSR and APTC information to the FFEs and SBE-FPs;

8. Facilitating payment of the initial premium amount to the appropriate QHP Issuer;

9. Facilitating an Enrollee's ability to disenroll from a QHP;

10. Educating Consumers, Applicants, Qualified Individuals or Enrollees—or these individuals' legal representatives or Authorized Representatives—on Insurance Affordability Programs and, if applicable, informing such individuals of eligibility for Medicaid or the Children's Health Insurance Program (CHIP);

11. Assisting an Enrollee in reporting changes in eligibility status to the FFEs and SBE-FPs throughout the coverage year, including changes that may affect eligibility (e.g., adding a dependent);

12. Correcting errors in the application for QHP enrollment;

13. Informing or reminding Enrollees when QHP coverage should be renewed, when Enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform Enrollees of QHP coverage options at renewal;

14. Providing appropriate information, materials, and programs to Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to inform and educate them about the use and management of their health information, as well as medical services and benefit options offered through the selected QHP or among the available QHP options;

15. Contacting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to assess their satisfaction or resolve complaints with services provided by EDE Entity in connection with the FFEs, SBE-FPs, EDE Entity, or QHPs;

16. Providing assistance in communicating with QHP Issuers;

17. Fulfilling the legal responsibilities related to the efficient functions of QHP Issuers in the FFEs and SBE-FPs, as permitted or required by a Web-broker EDE Entity's contractual relationships with QHP Issuers; and

18. Performing other functions substantially similar to those enumerated above and such other functions that CMS may approve in writing from time to time.

b. Collection of PII. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, EDE Entity may create, collect, disclose, access, maintain, store, and use the following PII from Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives— including, but not limited to:

- APTC percentage and amount applied
- Auto disenrollment information
- Applicant name
- Applicant address
- Applicant birthdate
- Applicant telephone number
- Applicant email
- Applicant Social Security Number
- Applicant spoken and written language preference
- Applicant Medicaid Eligibility indicator, start and end dates
- Applicant CHIP eligibility indicator, start and end dates
- Applicant QHP eligibility indicator, start and end dates
- Applicant APTC percentage and amount applied eligibility indicator, start and end dates
- Applicant household income
- Applicant maximum APTC amount
- Applicant CSR eligibility indicator, start and end dates
- Applicant CSR level
- Applicant QHP eligibility status change
- Applicant APTC eligibility status change
- Applicant CSR eligibility status change
- Applicant Initial or Annual Open Enrollment Indicator, start and end dates
- Applicant Special Enrollment Period ("SEP") eligibility indicator and reason code
- Contact name
- Contact address
- Contact birthdate
- Contact telephone number
- Contact email
- Contact spoken and written language preference
- Enrollment group history (past six months)
- Enrollment type period
- FFE Applicant ID
- FFE Member ID
- Issuer Member ID
- Net premium amount
- Premium amount, start and end dates

- Credit or Debit Card Number, name on card
- Checking account and routing number
- SEP reason
- Subscriber indicator and relationship to subscriber
- Tobacco use indicator and last date of tobacco use
- Custodial parent
- Health coverage
- American Indian/Alaska Native status and name of tribe
- Marital status
- Race/ethnicity
- Requesting financial assistance
- Responsible person
- Dependent name
- Applicant/dependent sex
- Student status
- Subscriber indicator and relationship to subscriber
- Total individual responsibility amount
- Immigration status
- Immigration document number
- Naturalization document number

c. Security and Privacy Controls. EDE Entity agrees to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including the NEE SSP. Furthermore, EDE Entity agrees to timely inform the Exchange of any material change in its administrative, technical, or operational environments, or any material change that would require an alteration of the privacy and security standards within this Agreement through the EDE Entity-initiated Change Request process (Section IX.c of this Agreement).

d. Use of PII. PII collected from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—in the context of completing an application for QHP, APTC, or CSR eligibility, if applicable, or enrolling in a QHP, or any data transmitted from or through the Hub, if applicable, may be used only for Authorized Functions specified in Section III.a of this Agreement. Such PII may not be used for purposes other than authorized by this Agreement or as consented to by a Consumer, Applicant, Qualified Individual, and Enrollee—or these individuals' legal representatives or Authorized Representatives.

e. Collection and Use of PII Provided Under Other Authorities. This Agreement does not preclude EDE Entity from collecting PII from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—for a non-FFE/non-SBE-FP/non-Hub purpose, and using, reusing, and disclosing PII obtained as permitted by applicable law and/or other applicable

authorities. Such PII must be stored separately from any PII collected in accordance with Section III.b of this Agreement.

f. Ability of Individuals to Limit Collection and Use of PII. EDE Entity agrees to provide the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—the opportunity to opt in to have EDE Entity collect, create, disclose, access, maintain, store, and use their PII. EDE Entity agrees to provide a mechanism through which the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—can limit the collection, creation, disclosure, access, maintenance, storage and use of his or her PII for the sole purpose of obtaining EDE Entity's assistance in performing Authorized Functions specified in Section III.a of this Agreement.

g. Downstream and Delegated Entities. EDE Entity will satisfy the requirement in 45 C.F.R. § 155.260(b)(2)(v) to require Downstream and Delegated Entities to adhere to the same privacy and security standards that apply to Non-Exchange Entities by entering into written agreements with any Downstream and Delegated Entities that will have access to PII collected in accordance with this Agreement. EDE Entity must require in writing all Downstream and Delegated Entities adhere to the terms of this Agreement.

   Upon request, EDE Entity must provide CMS with information about its downstream Agents/Brokers, EDE Entity's oversight of its downstream Agents/Brokers, and the EDE Environment(s) it provides to each of its downstream Agents/Brokers.

h. Commitment to Protect PII. EDE Entity shall not release, publish, or disclose Consumer, Applicant, Qualified Individual, or Enrollee PII to unauthorized personnel, and shall protect such information in accordance with provisions of any laws and regulations governing the adequate safeguarding of Consumer, Applicant, Qualified Individual, or Enrollee PII, the misuse of which carries with it the potential to cause financial, reputational, and other types of harm.

   1. Technical leads must be designated to facilitate direct contacts between the Parties to support the management and operation of the interconnection.

   2. The overall sensitivity level of data or information that will be made available or exchanged across the interconnection will be designated as MODERATE as determined by Federal Information Processing Standards (FIPS) Publication 199.

   3. EDE Entity agrees to comply with all federal laws and regulations regarding the handling of PII—regardless of where the organization is located or where the data are stored and accessed.

   4. EDE Entity's Rules of Behavior must be at least as stringent as the HHS Rules of Behavior.[3]

[3] The HHS Rules of Behavior are available at the following link: https://www.hhs.gov/ocio/policy/hhs-rob.html.

5. EDE Entity understands and agrees that all financial and legal liabilities arising from inappropriate disclosure or Breach of Consumer, Applicant, Qualified Individual, or Enrollee PII while such information is in the possession of EDE Entity shall be borne exclusively by EDE Entity.

6. EDE Entity shall train and monitor staff on the requirements related to the authorized use and sharing of PII with third parties and the consequences of unauthorized use or sharing of PII, and periodically audit their actual use and disclosure of PII.

IV. Effective Date and Term; Renewal.

a. Effective Date and Term. This Agreement becomes effective on the date the last of the two Parties executes this Agreement and ends the Day before the first Day of the open enrollment period ("OEP") under 45 C.F.R. § 155.410(e)(3) for the benefit year beginning January 1, 2025.

b. Renewal. This Agreement may be renewed upon the mutual agreement of the Parties for subsequent and consecutive one (1) year periods upon thirty (30) Days' advance written notice to EDE Entity.

V. Termination.

a. Termination without Cause. Either Party may terminate this Agreement without cause and for its convenience upon thirty (30) Days' prior written notice to the other Party.

EDE Entity must reference and complete the NEE Decommissioning Plan and NEE Decommissioning Close Out Letter in situations where EDE Entity will retire or decommission its EDE Environment.[4]

b. Termination of Agreement with Notice by CMS. The termination of this Agreement and the reconsideration of any such termination shall be governed by the termination and reconsideration standards adopted by the FFEs or SBE-FPs under 45 C.F.R. § 155.220. Notwithstanding the foregoing, EDE Entity shall be considered in "Habitual Default" of this Agreement in the event that it has been served with a non-compliance notice under 45 C.F.R. § 155.220(g) or an immediate suspension notice under Section V.c of this Agreement more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately terminate this Agreement upon notice to EDE Entity without any further opportunity to resolve the Breach and/or non-compliance.

c. Termination of Interconnection for Non-compliance. Instances of non-compliance with the privacy and security standards and operational requirements under this Agreement by EDE Entity, which may or may not rise to the level of a material Breach of this Agreement, may lead to termination of the interconnection between the Parties. CMS may block EDE Entity's access to CMS systems if EDE Entity does not

[4] The Non-Exchange Entity (NEE) Decommissioning Plan and NEE Decommissioning Close Out Letter are available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

implement reasonable precautions to prevent the risk of Security Incidents spreading to CMS' network or based on the existence of unmitigated privacy or security risks, or the misuse of the PII of Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives. In accordance with Section X.m of this Agreement, CMS is authorized to audit the security of EDE Entity's network and systems periodically by requesting that EDE Entity provide documentation of compliance with the privacy and security requirements in this Agreement and in the ISA. EDE Entity shall provide CMS access to its information technology resources impacted by this Agreement for the purposes of audits. CMS may suspend or terminate the interconnection if EDE Entity does not comply with such a compliance review request within seven (7) business days, or within such longer time period as determined by CMS. Further, notwithstanding Section V.b of this Agreement, CMS may immediately suspend EDE Entity's ability to transact information with the FFEs or SBE-FPs via use of its EDE Environment if CMS discovers circumstances that pose unacceptable or unmitigated risk to FFE operations or CMS information technology systems. If EDE Entity's ability to transact information with the FFEs or SBE-FPs is suspended, CMS will provide EDE Entity with written notice within two (2) business days.

d. Effect of Termination. Termination of this Agreement will result in termination of the functionality and electronic interconnection(s) covered by this Agreement, but will not affect obligations under EDE Entity's other respective agreement(s) with CMS, including the QHP Issuer Agreement, the Web-broker Agreement, or the Agent Broker General Agreement for Individual Market Federally-Facilitated Exchanges and State-Based Exchanges on the Federal Platform (Agent/Broker Agreement). However, the termination of EDE Entity's ISA, QHP Issuer Agreement, or Web-broker Agreement will result in termination of this Agreement and termination of EDE Entity's connection to CMS systems, including its connection to the Hub and ability to access the EDE suite of APIs as allowed by this Agreement. CMS may terminate this Agreement and EDE Entity's connection to CMS systems, consistent with this clause, if a Designated Representative, who is associated with the EDE Entity, has their Agent/Broker Agreement terminated by CMS.

e. Notice to Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—of Termination of the Interconnection/Agreement, Suspension of Interconnection, and Nonrenewal of Agreement. EDE Entity must provide Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—with written notice of termination of this Agreement without cause, as permitted under Section V.a of this Agreement, no less than ten (10) Days prior to the date of termination. Within ten (10) Days after termination or expiration of this Agreement or termination or suspension of the interconnection, EDE Entity must provide Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—with written notice of termination of this Agreement with cause under Section V.b of this Agreement; termination or suspension of the interconnection for non-compliance under Section V.c of this Agreement; termination resulting from termination of EDE Entity's ISA,

QHP Issuer Agreement, or Web-broker Agreement under Section V.d of this Agreement; or non-renewal of this Agreement.

The written notice required by this Section shall notify each Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—of the date the termination or suspension of the interconnection will or did occur and direct the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—to access his or her application through the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]) after that date. The written notice shall also provide sufficient details to the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—, including, but not limited to the Consumer's, Applicant's, Qualified Individual's, or Enrollee's Application ID, pending actions, and enrollment status, to allow the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—to update his or her application and provide the next steps necessary to update the Consumer's, Applicant's, Qualified Individual's, or Enrollee's application through the FFE. If EDE Entity's interconnection has been suspended, the written notice must also state that EDE Entity will provide updates to the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—regarding the Consumer's, Applicant's, Qualified Individual's, or Enrollee's—or these individuals' legal representatives or Authorized Representatives—ability to access his or her application through EDE Entity's website in the future.

In addition to providing written notice to Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—EDE Entity must also prominently display notice of the termination or suspension of the interconnection on EDE Entity's website, including language directing Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—to access their applications through the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]).

This clause will survive the expiration or termination of this Agreement.

f. Destruction of PII. EDE Entity covenants and agrees to destroy all PII in its possession at the end of the record retention period required under the NEE SSP. EDE Entity's duty to protect and maintain the privacy and security of PII, as provided for in the NEE SSP, shall continue in full force and effect until such PII is destroyed and shall survive the termination or expiration of this Agreement.

This clause will survive expiration or termination of this Agreement.

VI. Use of EDE Entity's EDE Environment by Agents, Brokers, or DE Entity Application Assisters.

a. General. EDE Entity may allow third-party Agents, Brokers, or DE Entity Application Assisters that are not or will not be a party to their own EDE Agreement with CMS to enroll Qualified Individuals in QHPs and to assist individuals in applying for APTC and CSRs through EDE Entity's EDE Environment. EDE Entity, or an Upstream EDE Entity,[5] for which EDE Entity provides an EDE Environment, must have a contractual and legally binding relationship with its third-party Agents, Brokers, or DE Entity Application Assisters reflected in a signed, written agreement between the third-party Agents, Brokers, or DE Entity Application Assisters and EDE Entity.

Except as provided in this Section, or as documented for CMS review and approval consistent with Section IX.c of this Agreement as a data connection in the ISA, EDE Entity may not establish a data connection between a third-party Agent's or Broker's website and the EDE Entity's EDE Environment that transmits any data.

The use of embedding tools and programming techniques, such as iframe technical implementations, which may enable the distortion, manipulation, or modification of the audited and approved EDE Environment and the overall EDE End-User Experience developed by a Primary EDE Entity, are prohibited unless explicitly approved through the EDE Entity-initiated Change Request process consistent with Section IX.c of this Agreement.

The EDE Entity environment must limit the number of concurrent sessions to one (1) session per a single set of credentials/FFE user ID. However, multiple sessions associated with a single set of credentials/FFE user ID that is traceable to a single device/browser is permitted.

b. Downstream White-Label Third-Party User Arrangement Requirements. Downstream third-party Agent and Broker arrangements may be Downstream White-Label Third-Party User Arrangements for which a Primary EDE Entity enables the third-party Agent or Broker to only make minor branding changes to the Primary EDE Entity's EDE Environment (i.e., adding an Agent's or Broker's logo or name to an EDE Environment). The use of embedding tools and programming techniques, such as iframe technical implementations, which may enable the distortion, manipulation, or modification of the audited and approved EDE Environment and the overall EDE End-User Experience developed by a Primary EDE Entity, are prohibited unless explicitly approved through the EDE Entity-initiated Change Request process consistent with Section IX.c of this Agreement.

c. Downstream White-Label Third-Party User Arrangement Data Exchange Limited Flexibility. With prior written approval from CMS, Downstream White-Label Third-Party User Arrangements may allow limited data collection from the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal

[5] Permissible Upstream EDE Entity arrangements are defined in Sections VIII.f, VIII.g, and VIII.h of this Agreement.

representatives or Authorized Representatives—on the Downstream third-party Agent's or Broker's website that can be used in the EDE End-User Experience via a one-way limited data connection to the Primary EDE Entity's EDE Environment. The following types of limited data collection by the third-party Agent's or Broker's website are permissible under this clause: 1) data to determine if a Consumer, Applicant, Qualified Individual, or Enrollee is (or should be) shopping for QHPs, such as basic information to assess potential eligibility for financial assistance, as well as to estimate premiums (e.g., household income, ages of household members, number of household members, and tobacco use status); and 2) data related to the Consumer's, Applicant's, Qualified Individual's, or Enrollee's service area (e.g., zip code, county, and State).

As part of the EDE-facilitated application and QHP enrollment processes, EDE Entity must not enable or allow the selection of QHPs by a Consumer or Agent/Broker on a third-party website that exists outside of the EDE Entity's approved DE Environment. This includes pre-populating or pre-selecting a QHP for a Consumer that was selected on a downstream Agent's/Broker's website or a lead generator's website. This prohibition does not extend to websites that are provided, owned, and maintained by entities subject to CMS regulations for QHP display (i.e., Web-brokers and QHP Issuers).

In any limited data collection arrangement, the data must be transmitted securely and in one direction only (i.e., from the downstream Agent or Broker to the Primary EDE Entity's EDE Environment). EDE Entity must not provide access to Consumer, Applicant, Qualified Individual, or Enrollee data to the third-party Agent or Broker outside of the EDE End-User Experience unless otherwise specified in Sections III.d, III.e, and III.f of this Agreement. Additionally, the Downstream White-Label Third-Party User Arrangement must not involve additional data exchanges beyond what is outlined above as permissible, which takes place in conjunction with the initial redirect prior to the beginning of the EDE End-User Experience on the Primary EDE Entity's EDE Environment.

d. Oversight Responsibilities. EDE Entity may only allow third-party Agents, Brokers, and DE Entity Application Assisters who are validly registered with the FFE for the applicable plan year to use its approved EDE Environment. EDE Entity must not provide access to its approved EDE Environment, the EDE End-User Experience or any data obtained via the EDE End-User Experience to an Agent or Broker until the Agent or Broker has completed the process for Agent or Broker Identity Proofing consistent with the requirements in Section IX.r of this Agreement.

VII. QHP Issuer Use of an EDE Environment.

QHP Issuer EDE Entities, operating as Primary EDE Entities or Upstream EDE Entities, must bind all affiliated Issuer organizations (i.e., HIOS IDs) that use its EDE Environment or EDE End-User Experience—either for Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—use or Agent or Broker use—to the terms and provisions of this Agreement. QHP Issuer EDE Entities must identify all applicable affiliated Issuer organizations that will use its EDE Environment during the

onboarding process in the "Operational and Oversight Information" form provided by CMS[6]. The signatory of this Agreement on behalf of the QHP Issuer EDE Entity must have sufficient authority to execute an agreement with CMS on behalf of the QHP Issuer EDE Entity and all affiliated QHP Issuer organizations that use the QHP Issuer EDE Entity's EDE Environment or EDE End-User Experience. QHP Issuer EDE Entities must identify all applicable affiliated QHP Issuer organizations in the "Operational and Oversight Information" form provided by CMS.

VIII. Audit Requirements.

a. Operational Readiness Review ("ORR"). In order to receive approval to participate in EDE and utilize an integrated EDE Environment, EDE Entity must contract with one or more independent Auditor(s) consistent with this Agreement's provisions and applicable regulatory requirements to conduct an ORR, composed of a business requirements audit and a privacy and security audit.[7] EDE Entity must follow the detailed guidance CMS provided in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.[8]

The Auditor must document and attest in the ORR report that EDE Entity's EDE Environment, including its website and operations, complies with the terms of this Agreement, the ISA, EDE Entity's respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement), the Framework for the Independent Assessment of Security and Privacy Controls for Enhanced Direct Enrollment Entities,[9] and applicable program requirements. If an EDE Entity will offer its EDE Environment in a State in which a non-English language is spoken by a Limited English Proficient (LEP) population that reaches ten (10) percent or more of the State's population, as determined in guidance published by the Secretary of HHS,[10] the Auditor conducting EDE Entity's business requirements audit must also audit the non-English language version of the application user interface (UI) and any critical communications EDE Entity sends Consumers, Applicants, Qualified Individuals, or Enrollee —or these individuals' legal representatives or Authorized Representatives—in relation to their use of its EDE Environment for compliance with

[6] The Operational and Oversight Information form is available in the PY 2023 DE Documentation Package zip file on CMS zONE at the following link: https://zone.cms.gov/document/business-audit.
[7] The Auditor must use NIST SP 800-53A, which describes the appropriate assessment procedure (examine, interview, and test) for each control to evaluate that the control is effectively implemented and operating as intended.
[8] This document is available at the following link: https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf.
[9] This document is available at the following link within the Privacy and Security Templates Resources: https://zone.cms.gov/document/privacy-and-security-audit.
[10] Guidance and Population Data for Exchanges, Qualified Health Plan Issuers, and Web-Brokers to Ensure Meaningful Access by Limited-English Proficient Speakers Under 45 CFR §155.205(c) and §156.250 (March 30, 2016) https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Language-access-guidance.pdf and "Appendix A- Top 15 Non-English Languages by State" https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508_update12-20-16.pdf. HHS may release revised guidance. DE Entity should refer to the most current HHS guidance.

applicable CMS requirements. EDE Entity must submit the resulting business requirements and privacy and security audit packages to CMS.

The ORR must detail EDE Entity's compliance with the requirements set forth in Appendix C, including any requirements set forth in CMS guidance referenced in Appendix C.[11] The business requirements and privacy and security audit packages EDE Entity submits to CMS must demonstrate that EDE Entity's Auditor(s) conducted its review in accordance with the review standards set forth in Appendix C and in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements.

CMS will approve EDE Entity's EDE Environment only once it has reviewed and approved the business requirements audit and privacy and security audit findings reports. Final approval of EDE Entity's EDE Environment will be evidenced by CMS countersigning the ISA with EDE Entity. Upon receipt of the counter-signed ISA, EDE Entity will be approved to use its approved EDE Environment consistent with applicable regulations, this Agreement, and the ISA.

b. Identification of Auditor(s) and Subcontractors of Auditor(s). All Auditor(s), including any Auditor(s) that has subcontracted with EDE Entity's Auditor(s), will be considered Downstream or Delegated Entities of EDE Entity pursuant to EDE Entity's respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement) and applicable program requirements. EDE Entity must identify each Auditor it selects, and any subcontractor(s) of the Auditor(s), in Appendix E of this Agreement. EDE Entity must also submit a copy of the signed agreement or contract between the Auditor(s) and EDE Entity to CMS.

c. Conflict of Interest. For any arrangement between EDE Entity and an Auditor for audit purposes covered by this Agreement, EDE Entity must select an Auditor that is free from any real or perceived conflict(s) of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. EDE Entity must disclose to HHS any financial relationships between the Auditor, and individuals who own or are employed by the Auditor, and individuals who own or are employed by an EDE Entity for which the Auditor is conducting an ORR pursuant to 45 C.F.R. §§ 155.221(b)(4) and (f). EDE Entity must document and disclose any conflict(s) of interest in the form in Appendix F, if applicable.

d. Auditor Independence and Objectivity. EDE Entity's Auditor(s) must remain independent and objective throughout the audit process for both audits. An Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the EDE Environment and the determination of security and privacy control effectiveness or business requirement compliance. EDE Entity must not take any actions that impair

[11] The table in Appendix C is an updated version of Exhibit 2 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

the independence and objectivity of EDE Entity's Auditor. EDE Entity's Auditor must attest to their independence and objectivity in completing the EDE audit(s).

e. Required Documentation. EDE Entity must maintain and/or submit the required documentation detailed in Appendix D, including templates provided by CMS, to CMS in the manner specified in Appendix D.[12] Documentation that EDE Entity must submit to CMS (as set forth in Appendix D) will constitute EDE Entity's EDE Application.

f. Use of an EDE Environment by a QHP Issuer with Minor Branding Deviations (White-Label Issuer Upstream EDE Entity).

A QHP Issuer EDE Entity may use an approved EDE Environment provided by a Primary EDE Entity. If a QHP Issuer EDE Entity implements and uses an EDE Environment that is identical to its Primary EDE Entity's EDE Environment, except for minor deviations for branding or QHP display changes relevant to the Issuer's QHPs, the QHP Issuer EDE Entity is not required to submit a business requirements audit package and privacy and security audit package. CMS refers to a QHP Issuer EDE Entity operating consistent with this Section as a White-Label Issuer Upstream EDE Entity. In all arrangements permitted under this Section, all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions specified in Section III.a of this Agreement must be conducted within the confines of the Primary EDE Entity's approved EDE Environment.

In all arrangements permitted under this Section, the White-Label Issuer Upstream EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265 and 156.1230, operational requirements, this Agreement, and the ISA. Any Primary EDE Entity supplying an EDE Environment to a White-Label Issuer Upstream EDE Entity will be considered a Downstream or Delegated Entity of the White-Label Issuer Upstream EDE Entity. A White-Label Issuer Upstream EDE Entity must identify its Primary EDE Entity in the "Operational and Oversight Information" form provided by CMS . A White-Label Issuer Upstream EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the White-Label Issuer Upstream EDE Entity and the Primary EDE Entity.

g. Use of an EDE Environment by a QHP Issuer with Additional Functionality or Systems (Hybrid Issuer Upstream EDE Entity).

If a QHP Issuer EDE Entity will implement its own EDE Environment composed, in part, of an approved EDE Environment provided by a Primary EDE Entity and, in

[12] The table in Appendix D is a combined version of Exhibits 4 and 7 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

part, of additional functionality or systems implemented by or on behalf of the QHP Issuer EDE Entity, the QHP Issuer EDE Entity may be required to retain an Auditor to conduct part(s) of the ORR relevant to functionalities and systems implemented by the QHP Issuer EDE Entity outside of the Primary EDE Entity's EDE Environment, or in addition to the Primary EDE Entity's approved EDE Environment, and to analyze the effect, if any, of those functionalities and systems on the operations and compliance of the Primary EDE Entity's approved EDE Environment. CMS refers to a QHP Issuer EDE Entity operating consistent with this Section as a Hybrid Issuer Upstream EDE Entity. In this scenario, the Hybrid Issuer Upstream EDE Entity may be required to submit to CMS an ORR audit package that contains the results of the supplemental business requirements audit and/or privacy and security audit, as appropriate, in which the Auditor reviewed the additional functionality or systems implemented by or on behalf of the Hybrid Issuer Upstream EDE Entity. The Hybrid Issuer Upstream EDE Entity may be required to submit to CMS an ORR consisting of the results of its Auditor's review of its implementation of non-inheritable, Hybrid and inheritable but not inherited EDE privacy and security controls. The ORR audit package that contains the results of the business requirements audit and/or privacy and security audit covering additional functionality or systems implemented by or on behalf of the Hybrid Issuer Upstream EDE Entity must demonstrate the Hybrid Issuer Upstream EDE Entity's compliance with applicable regulations, operational requirements, this Agreement, and the ISA. The Hybrid Issuer Upstream EDE Entity does not need to submit the Primary EDE Entity's ORR.

CMS considers any changes to the Primary EDE Entity's approved EDE Environment or the overall EDE End-User Experience—beyond minor deviations for branding or QHP display changes relevant to the Issuer's QHPs—to be the addition of functionality or systems to an approved EDE Environment subject to the requirements of this Section.

CMS has identified the following non-exclusive list as additional functionality that requires a supplemental audit submission:

1. Hybrid Issuer Upstream EDE Entities implementing a single sign-on (SSO) solution must retain an Auditor to conduct a supplemental security and privacy audit and submit the results to CMS consistent with the EDE Guidelines.[13]

In all arrangements permitted under this paragraph, the Hybrid Issuer Upstream EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265, and 156.1230, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements for Issuers as defined in 45 C.F.R. §§ 155.221, 156.265 and 156.1230, operational requirements, this Agreement, and the ISA. Any

[13] A Hybrid Issuer Upstream EDE Entity implementing a SSO solution may leverage prior audit results that assessed some or all control requirements listed in Exhibit 14 of the EDE Guidelines, available at the following link: https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf if the prior audit was conducted within one year of the date of submission of the audit documentation to CMS.

Primary EDE Entity supplying an EDE Environment to the Hybrid Issuer Upstream EDE Entity will be considered a Downstream or Delegated Entity of the Hybrid Issuer Upstream EDE Entity. A Hybrid Issuer Upstream EDE Entity must identify its Primary EDE Entity in the "Operational and Oversight Information" form provided by CMS . The Hybrid Issuer Upstream EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the Hybrid Issuer Upstream EDE Entity and the Primary EDE Entity. The Primary EDE Entity must identify inheritable Common Controls and Hybrid Controls that the Hybrid Issuer Upstream EDE Entity should leverage. The inherited Common Controls and Hybrid Controls must be documented in the NEE SSP Template and must also be documented as part of the written contract between the Primary EDE Entity and the Hybrid Issuer Upstream EDE Entity.

A Hybrid Issuer Upstream EDE Entity operating under this provision cannot provide access to its EDE Environment to another Issuer or a Hybrid Non-Issuer Upstream EDE Entity.

h. Use of an EDE Environment by a Non-Issuer Entity with Additional Functionality or Systems (Hybrid Non-Issuer Upstream EDE Entity).

If a Hybrid Non-Issuer Upstream EDE Entity will implement its own EDE Environment composed, in part, of an approved EDE Environment provided by a Primary EDE Entity and, in part, of additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer Upstream EDE Entity, the Hybrid Non-Issuer EDE Entity must retain an Auditor to conduct part(s) of the ORR relevant to functionalities and systems implemented by the Hybrid Non-Issuer EDE Entity outside of the Primary EDE Entity's EDE Environment, or in addition to the Primary EDE Entity's approved EDE Environment, and to analyze the effect, if any, of those functionalities and systems on the operations and compliance of the Primary EDE Entity's approved EDE Environment.[14] In this scenario, the Hybrid Non-Issuer EDE Entity must submit an ORR consisting of the results of its Auditor's review of its implementation of non-inheritable, Hybrid and inheritable but not inherited EDE privacy and security controls. The Hybrid Non-Issuer EDE Entity may also be required to submit to CMS a supplemental ORR audit package that contains the results of any supplemental business requirements and/or privacy and security audits, as appropriate, in which the Auditor reviewed the additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer EDE Entity.[15] The ORR, and

[14] With respect to Agents and Brokers regulated by this section as Hybrid Non-Issuer Upstream EDE Entities, these arrangements are distinct and independent from those arrangements regulated under Section VI of this Agreement. An Agent or Broker in a limited data-sharing arrangement consistent with Section VI.c of this Agreement would not necessarily also be subject to the requirements for Hybrid Non-Issuer Upstream EDE Entities under Section VIII.h of this Agreement. The determination of what requirements apply to a particular arrangement will be a fact heavy analysis that takes into account the specific details of the arrangement.

[15] A Hybrid Non-Issuer Upstream EDE Entity may leverage prior audit results that assessed some or all control requirements listed in Exhibit 12 and Exhibit 13 of Appendix A of the EDE Guidelines, if the prior audit was conducted within one year of the date of submission of the audit documentation to CMS. The EDE Guidelines are available at the following link: https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf.

supplemental ORR audit package that contains the results of the supplemental business requirements audit and/or privacy and security audit covering additional functionality or systems implemented by or on behalf of the Hybrid Non-Issuer EDE Entity (when required), must demonstrate the Hybrid Non-Issuer EDE Entity's compliance with applicable regulations, operational requirements, this Agreement, and the ISA. The Hybrid Non-Issuer EDE Entity does not need to submit the Primary EDE Entity's ORR.

CMS considers any changes to the Primary EDE Entity's approved EDE Environment or the overall EDE End-User Experience beyond minor deviations for branding to be the addition of functionality or systems to an approved EDE Environment subject to the requirements of this Section. In all arrangements permitted under this paragraph, the Hybrid Non-Issuer EDE Entity is responsible for compliance with all of the requirements contained in all applicable regulations and guidance, as well as in this Agreement. This includes oversight of the Primary EDE Entity and ensuring its Primary EDE Entity's EDE Environment complies with all applicable regulations, including QHP display requirements as defined in 45 C.F.R. §§ 155.220(c) and 155.221, operational requirements, this Agreement, and the ISA. Any Primary EDE Entity supplying an EDE Environment to the Hybrid Non-Issuer EDE Entity will be considered a Downstream or Delegated Entity of the Hybrid Non-Issuer EDE Entity. A Hybrid Non-Issuer EDE Entity must identify its Primary EDE Entity in the "Operational and Oversight Information" form provided by CMS. The Hybrid Non-Issuer EDE Entity must have a contractual and legally binding relationship with its Primary EDE Entity reflected in a signed, written agreement between the Hybrid Non-Issuer EDE Entity and the Primary EDE Entity. The Primary EDE Entity must identify inheritable Common Controls and Hybrid Controls that the Hybrid Non-Issuer EDE Entity should leverage. The inherited Common Controls and Hybrid Controls must be documented in the NEE SSP Template and must also be documented as part of the written contract between the Primary EDE Entity and the Hybrid Non-Issuer EDE Entity.

Depending on the additional functionality and systems added, the Hybrid Non-Issuer EDE Entity may also need to onboard and register with CMS as a Web-broker. For example, a Hybrid Non-Issuer EDE Entity that hosts its own QHP display or plan shopping experience as part of the EDE End-User Experience must be registered with CMS as a Web-broker.

The QHP display or plan shopping experience displayed in the EDE End-User Experience provided to or operated by a Hybrid Non-Issuer EDE Entity must comply with the requirements of 45 C.F.R. §§ 155.220 and 155.221.

When onboarding, annually during agreement renewal, and upon request, the Hybrid Non-Issuer EDE Entity must provide CMS operational information, including, but not limited to, its Designated Representative's National Producer Number (NPN), State licensure information, and information about its downstream agents/brokers, if applicable. The Designated Representative designated by the Hybrid Non-Issuer EDE

Entity must have completed registration and, if applicable, training with the FFE consistent with 45 C.F.R. § 155.220(d).

A Hybrid Non-Issuer EDE Entity operating under this provision cannot provide access to its EDE Environment to an Issuer or another Hybrid Non-Issuer Upstream EDE Entity.

IX. FFE Eligibility Application and Enrollment Requirements.

a. FFE Eligibility Application End-State Phases and Phase-Dependent Screener Questions. Appendix G describes each of the three end-state phases for hosting applications using the EDE Pathway (Phase 1, Phase 2, and Phase 3).[16] EDE Entity must select and implement an end-state phase. If EDE Entity has selected application end-state Phase 1 or Phase 2, it must implement the requirements related to phase-dependent screener questions set forth in Appendix C. In addition, EDE Entity must meet any end-state phase-related communications requirements established by CMS. EDE Entity must indicate the phase it has selected in the "Operational and Oversight Information" form provided by CMS.

The business requirements audit package EDE Entity submits to CMS must demonstrate that EDE Entity's EDE Environment meets all requirements associated with EDE Entity's selected phase, as set forth in Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements,[17] Enhanced Direct Enrollment API Companion Guide,[18] and FFE UI Application Principles for Integration with FFE APIs.[19] EDE Entity must consult CMS prior to switching phases. If EDE Entity decides to switch to a different phase after its Auditor has completed the business requirements audit, EDE Entity's Auditor must conduct portions of a revised business requirements audit to account for the changes to the EDE Environment necessary to implement the new end-state phase selected by EDE Entity to confirm compliance with all applicable requirements.

b. EDE Entity Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—Support for Term of Agreement. EDE Entity's EDE Environment must support Consumer-, Applicant-, Qualified Individual-, or Enrollee—or these individuals' legal representatives or Authorized Representatives—reported Changes in Circumstances (CiCs), inclusive of SEP CiCs and non-SEP CiCs, and SEPs within EDE Entity's chosen end-state phase for the full term of this Agreement, as well as supporting re-enrollment application activities. Furthermore, all EDE Entities, regardless of the phase chosen, must support households that wish to enroll in more than one enrollment group. Consistent with the general expectations for EDE requirements—that the EDE requirements are

[16] The table in Appendix G is an updated version of Exhibit 3 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."
[17] See supra note 8.
[18] The document Enhanced Direct Enrollment API Companion *Guide* is available at the following link: https://zone.cms.gov/document/api-information.
[19] The document FFE UI Application Principles for Integration with FFE APIs is available at the following link: https://zone.cms.gov/document/eligibility-information.

implemented for and provided to all users of an EDE Environment—Primary EDE Entities must provide the functionalities described in this paragraph for all users of the Primary EDE Entity's EDE Environment, including any Upstream EDE Entities and their users (e.g., Downstream Agents and Brokers).

If EDE Entity is no longer operating an EDE Environment, EDE Entity must direct the Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—to the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]). EDE Entity should take reasonable steps to continue supporting households that have used their EDE Environment in the past to transfer to the new EDE Pathway. CMS suggests that reasonable steps would include: send written notices to Consumers of the steps to create an account/transfer their account to the different Primary EDE Entity, provide the requisite information for them to create an account on that other site or carry their information to a different pathway, and provide a notice on the site that EDE Entity has transitioned its EDE Pathway to a different environment. EDE Entity can go beyond these limited, minimum requirements in easing the Consumer transition to [New Entity] and should follow the EDE Entity-initiated Change Request process as described in Section IX.c of this Agreement for this functionality as appropriate

This provision survives the termination of the Agreement.

c. EDE Entity-initiated Modifications to EDE Environment (EDE Entity-initiated Change Requests and EDE Entity-initiated Phase Change Requests). EDE Entity must notify CMS immediately if it intends to make any change to its audited or approved EDE Environment, including when EDE Entity opts to change to a different EDE application phase (from its approved or audited EDE phase), consistent with the processes and standards defined by CMS in the Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems.[20] CMS excludes changes made in response to an Auditor's documented findings (if the findings were submitted to CMS), to CMS technical assistance, or to resolve compliance findings from being subject to the procedures detailed in the Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems.

d. CMS-initiated Modifications to EDE Program Requirements (CMS-initiated Change Requests). CMS will periodically release updates to EDE program requirements in the form of CMS-initiated Change Requests (CRs); these CMS-initiated CRs are documented in the EDE Change Request Tracker.[21] EDE Entity must provide specified documentation to CMS demonstrating its implementation of applicable CMS-initiated CRs by the CMS-established deadline. EDE Entity must make any CMS-mandated changes within the timeline established by CMS to make such changes. If an EDE Entity does not timely submit documentation of its

[20] The document Change Notification Procedures for Enhanced Direct Enrollment Information Technology Systems is available at the following link: https://zone.cms.gov/document/business-audit.
[21] The EDE Change Request Tracker is located on CMS zONE: https://zone.cms.gov/document/business-audit.

implementation of such CRs, CMS may suspend the non-compliant EDE Entity's access to the EDE Pathway.

e. Maintenance of an Accurate Testing Environment. EDE Entity must maintain a testing environment that accurately represents the EDE Entity's production environment and integration with the EDE Pathway, including functional use of all EDE APIs. Approved and Prospective Phase Change EDE Entities must maintain at least one testing environment that reflects their current production EDE environments when developing and testing any prospective changes to their production EDE environments. This will require Approved and Prospective Phase Change EDE Entities to develop one or more separate environments (other than production and the testing environment that reflects production) for developing and testing prospective changes to their production environments. Network traffic into and out of all non-production environments is only permitted to facilitate system testing and must be restricted by source and destination access control lists, as well as ports and protocols, as documented in the NEE SSP, SA-11 implementation standard. The EDE Entity shall not submit actual PII to the FFE Testing Environments. The EDE Entity shall not submit test data to the FFE Production Environments. The EDE Entity's testing environments shall be readily accessible to applicable CMS staff and contractors via the Internet to complete CMS audits.

   EDE Entity must provide CMS, via the DE Help Desk, with a set of credentials and any additional instructions necessary so that CMS can access the testing environment that reflects the EDE Entity's production environment to complete audits of the EDE Entity's EDE Environment. EDE Entity must ensure that the testing credentials are valid and that all APIs and components of the EDE Environment in the testing environment, including the remote identity proofing (RIDP) services, are accessible for CMS to audit EDE Entity's EDE Environment as determined necessary by CMS.

f. Penetration Testing. The EDE Entity must conduct penetration testing which examines the network, application, device, and physical security of its EDE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Before conducting the penetration testing, the EDE Entity must execute a Rules of Engagement with their Auditor's penetration testing team. The EDE Entity must also notify their CMS designated technical counterparts on their annual penetration testing schedule a minimum of five (5) business days prior to initiation of the penetration testing using the CMS-provided form.[22] During the penetration testing, the Auditor's testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment. The penetration testing shall be conducted in the lower environment that reflects the EDE Entity's current production environment, consistent with Section IX.e.

[22] The Penetration Testing Notification Form is available at the following links: https://zone.cms.gov/document/privacy-and-security-audit.

g. Identity Proofing. EDE Entity must meet the identity proofing implementation requirements set forth in Appendix C.

h. Accurate and Streamlined Eligibility Application UI. EDE Entity must meet the accurate and streamlined eligibility application UI requirements set forth in Appendix C.

i. Post-Eligibility Application Communications. EDE Entity must provide account management functions for Consumers, Applicants, Qualified Individuals, or Enrollees —or these individuals' legal representatives or Authorized Representatives— and timely communicate with Consumers, Applicants, Qualified Individuals, or Enrollees —or these individuals' legal representatives or Authorized Representatives— regarding their application and coverage status. EDE Entity must meet all requirements related to post-eligibility application communications and account management functions set forth in Appendix C. In addition to those requirements, EDE Entity must update and report changes to the Consumer's, Applicant's, Qualified Individual's, or Enrollee's application and enrollment information to the FFE and must comply with future CMS guidance that elaborates upon EDE Entity's duties under this Agreement and applicable regulations.

j. Accurate Information About Exchanges and Consumer, Applicant, Qualified Individual, or Enrollee Communications. EDE Entity must meet the requirements related to providing to Consumers, Applicants, Qualified Individuals, or Enrollees— or these individuals' legal representatives or Authorized Representatives—accurate information about Exchanges and the Consumer, Applicant, Qualified Individual, or Enrollee communications requirements set forth in Appendix C. In addition, EDE Entity must meet the marketing-related communications requirements defined by CMS in the Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements and the Communications Toolkit.[23]

k. Documentation of Interactions with Consumer, Applicant, Qualified Individual, or Enrollee Applications or the Exchange. EDE Entity must meet the requirements related to documentation of interactions with Consumer, Applicant, Qualified Individual, or Enrollee applications or the Exchange set forth in Appendix C.

l. Eligibility Results Testing and Standalone Eligibility Service (SES) Testing. EDE Entity must meet the requirements related to eligibility results testing and SES testing set forth in Appendix C.

m. API Functional Integration Requirements. EDE Entity must meet the API functional integration requirements set forth in Appendix C.

n. Application UI Validation. EDE Entity must meet the application UI validation requirements set forth in Appendix C.

[23] The Communications Toolkit is stored within the Business Report Template and Toolkits file available at the following link: https://zone.cms.gov/document/business-audit.

o. Section 508-compliant UI. EDE Entity must meet the 508-compliant UI requirements set forth in Appendix C.

p. Non-English-Language Version of the Application UI and Communication Materials. EDE Entity must translate the Application UI and any critical communications EDE Entity sends Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—in relation to their use of its EDE Environment into any non-English language that is spoken by an LEP population that reaches ten percent or more of the population of the relevant State as set forth in Appendix C.

q. Correction of Consumer, Applicant, Qualified Individual, or Enrollee Application Information. If EDE Entity identifies issues in its EDE Environment constituting noncompliance with the EDE program requirements as documented in Section IX of this Agreement that may affect the accuracy of a Consumer's, Applicant's, Qualified Individual's, or Enrollee's Application Information—including the Exchange's eligibility determination or enrollment status—EDE Entity must notify CMS immediately by email to directenrollment@cms.hhs.gov. For any such issues identified by EDE Entity or CMS, EDE Entity must provide CMS-requested data on a timeline established by CMS. CMS-requested data includes all data that CMS deems necessary to determine the scope of the issues and identify potentially affected Consumers, Applicants, Qualified Individuals, or Enrollees, including records maintained by EDE Entity consistent with Section IX.k of this Agreement. EDE Entity must provide assistance to CMS to identify the population of Consumers, Applicants, Qualified Individuals, or Enrollees potentially affected by the identified issues. EDE Entity must remedy CMS- or EDE Entity-identified issues in EDE Entity's EDE Environment in a manner and timeline subject to CMS' approval. CMS may require that EDE Entity submit updated application information within thirty (30) Days to correct inaccuracies in previously submitted applications. CMS may require that EDE Entity conduct necessary CMS-approved outreach to notify the potentially affected Consumers, Applicants, Qualified Individuals, or Enrollees of any action required by the Consumers, Applicants, Qualified Individuals, or Enrollees, if applicable, and of any changes in eligibility or enrollment status as a result of the issues.

r. Agent/Broker Identity Proofing Requirements. EDE Entity must implement Agent and Broker identity verification procedures that consist of the following requirements:

1. EDE Entity must provide the User ID of the requester in each EDE API call. For Agents and Brokers, the User ID must exactly match the FFE-assigned User-ID for the Agent or Broker using the EDE Environment or the request will fail FFE User ID validation.[24] As a reminder, for Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—the User ID should be the account User ID for the

[24] In order for an Agent or Broker to obtain and maintain an FFE User ID, the Agent or Broker must complete registration and training with the Exchange annually.

Consumer, Applicant, Qualified Individual, or Enrollee or a distinct identifier for the Consumer, Applicant, Qualified Individual, or Enrollee.

2. EDE Entity must identity proof all Agents and Brokers prior to allowing the Agents and Brokers to use the EDE Environment. EDE Entity may conduct identity proofing in one of the following ways:

    a. Use the FFE-provided Remote Identity Proofing/Fraud Solutions Archive Reporting Service (RIDP/FARS) or a Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS)-approved service to remotely identity-proof Agents and Brokers; OR

    b. Manually identity-proof Agents and Brokers following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing."[25]

3. EDE Entity must validate an Agent's or Broker's National Producer number (NPN) using the National Insurance Producer Registry (https://www.nipr.com) prior to allowing the Agent or Broker to use the EDE Environment.

4. EDE Entity must review the Agent/Broker Suspension and Termination list prior to allowing the Agent or Broker to initially use the EDE Environment.[26]

5. If EDE Entity does not provide Agent or Broker identity proofing functionality consistent with the requirements above, EDE Entity cannot provide access to its EDE Environment to third-party Agents or Brokers. Furthermore, if a Primary EDE Entity does not provide Agent or Broker identity proofing functionality consistent with the requirements above, any Upstream EDE Entities that wish to use the Agent or Broker EDE Pathway must implement an Agent or Broker identity proofing approach consistent with these requirements prior to offering Agents or Brokers access to their EDE Environments. In such cases, the Upstream EDE Entities must contract with an independent Auditor to conduct an audit to evaluate the Agent or Broker identity proofing requirements consistent with this Section, and submit the audit to CMS for approval.

6. EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3.

7. EDE Entity must not permit Agents and Brokers using the EDE Environment to share access control credentials.

s. Implement Full EDE API Suite of Required Services. EDE Entity must implement the full EDE API suite of required services, regardless of EDE Entity's chosen application end-state phase. The suite of required services consists of the following APIs: Store ID Proofing, Person Search, Create App, Create App from Prior Year

[25] The document Acceptable Documentation for Identity Proofing is available on CMS zONE at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.
[26] The Agent/Broker Suspension and Termination List is available at: https://data.healthcare.gov/ab-suspension-and-termination-list.

App, Store Permission, Revoke Permission, Get App, Add Member, Remove Member, Update App, Submit App, Get Data Matching Issue (DMI), Get Special Enrollment Period Verification Issue (SVI), Metadata Search, Notice Retrieval, Submit Enrollment, Document Upload, System and State Reference Data, Get Enrollment, Payment Redirect[27], Update Policy, and Event-Based Processing (EBP). CMS may release additional required or optional APIs during the term of this Agreement. If CMS releases a required API, the change will be considered a CMS-initiated Change Request consistent with Section IX.d of this Agreement.

t. Maintain Full EDE API Suite of Required Services. In addition to any CMS-initiated Change Requests, CMS may make technical updates to Exchange systems or APIs that may affect EDE Entity's use of the EDE APIs. In order to maintain a functional EDE Environment and avoid errors or discrepancies when submitting data to and receiving data from the Exchange, EDE Entity must maintain an EDE Environment that implements changes as needed and documented in EDE technical documentation provided by CMS.[28]

u. Health Reimbursement Arrangement (HRA) Offer Disclaimer. EDE Entity must implement disclaimers for Qualified Individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the Qualified Individuals consistent with CMS guidance. Disclaimers for various scenarios are detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.[29]

v. Inactive, Approved Primary EDE Entities to Demonstrate Operational Readiness and Compliance. In order for an approved Primary EDE Entity to maintain status as an approved Primary EDE Entity during the annual renewal process for this Agreement, EDE Entity must demonstrate a history of enrollments completed via EDE during the term of the prior year's Agreement if the approved Primary EDE Entity has been approved for at least one year as determined by the date of the initial approval of the Primary EDE Entity and initial execution of the ISA. If the EDE Entity has been approved for at least one year and does not have a history of enrollments completed via EDE during the term of the prior year's Agreement, EDE Entity must demonstrate operational readiness and compliance with applicable requirements as documented in the EDE Guidelines in order to continue to participate as an approved Primary EDE Entity. Under this section, CMS may withhold execution of the subsequent plan year's Agreement and ISA or delay approval of an Upstream EDE Entity until EDE Entity has demonstrated operational readiness and compliance with applicable requirements to CMS's satisfaction.

[27] For information on exceptions to the requirement for EDE Entities to integrate with the Payment Redirect API, see Section 13.3, Payment Redirect Integration Requirements, of the EDE API Companion Guide, available at the following link: https://zone.cms.gov/document/api-information.

[28] EDE APIs technical documentation is available on CMS zONE at the following link: https://zone.cms.gov/document/api-information.

[29] The document Direct Enrollment API Specs is available on CMS zONE at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

X. Miscellaneous.

a. Notice. All notices to Parties specifically required under this Agreement shall be given in writing and shall be delivered as follows:

If to CMS:

By email:
directenrollment@cms.hhs.gov

By mail:
Centers for Medicare & Medicaid Services (CMS)
Center for Consumer Information and Insurance Oversight (CCIIO)
Attn: Office of the Director
Room 739H
200 Independence Avenue, SW
Washington, DC 20201

If to EDE Entity, to EDE Entity's primary contact's email address on record.

Notices sent by hand or overnight courier service, or mailed by certified or registered mail, shall be deemed to have been given when received; notices sent by email shall be deemed to have been given when the appropriate confirmation of receipt has been received; provided that notices not given on a business day (i.e., Monday-Friday excluding federal holidays) between 9:00 a.m. and 5:00 p.m. local time where the recipient is located shall be deemed to have been given at 9:00 a.m. on the next business day for the recipient. A Party to this Agreement may change its contact information for notices and other communications by providing written notice of such changes in accordance with this provision. Such notice should be provided thirty (30) Days in advance of such change, unless circumstances warrant a shorter timeframe.

b. Assignment and Subcontracting. Except as otherwise provided in this Section, EDE Entity shall not assign this Agreement in whole or in part, whether by merger, acquisition, consolidated, reorganization, or otherwise any portion of the services to be provided by EDE Entity under this Agreement without the express, prior written consent of CMS, which consent may be withheld, conditioned, granted, or denied in CMS' sole discretion. EDE Entity must provide written notice at least thirty (30) Days prior to any such proposed assignment, including any change in ownership of EDE Entity or any change in management or ownership of the EDE Environment. Notwithstanding the foregoing, CMS does not require prior written consent for subcontracting arrangements that do not involve the operation, management, or control of the EDE Environment. EDE Entity must report all subcontracting arrangements on its annual Operational and Oversight Information form during the annual EDE Agreement Renewal process and submit revisions annually thereafter. EDE Entity shall assume ultimate responsibility for all services and functions described under this Agreement, including those that are subcontracted to other entities, and must ensure that subcontractors will perform all functions in accordance with all applicable requirements. EDE Entity shall further be subject to such oversight and enforcement actions for functions or activities performed by subcontractors as may otherwise be provided for under applicable law and program requirements,

including EDE Entity's respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement). Notwithstanding any subcontracting of any responsibility under this Agreement, EDE Entity shall not be released from any of its performance or compliance obligations hereunder, and shall remain fully bound to the terms and conditions of this Agreement as unaltered and unaffected by such subcontracting.

If EDE Entity attempts to make an assignment, subcontracting arrangement or otherwise delegate its obligations hereunder in violation of this provision, such assignment, subcontract, or delegation shall be deemed void *ab initio* and of no force or effect, and EDE Entity shall remain legally bound hereto and responsible for all obligations under this Agreement.

c. Use of the FFE Web Services. EDE Entity will only use a CMS-approved EDE Environment when accessing the APIs and web services that facilitate EDE functionality to enroll Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix H.

d. Incident Reporting Procedures: EDE Entity must implement Incident and Breach Handling procedures as required by the NEE SSP and that are consistent with CMS's Incident and Breach Notification Procedures. Such policies and procedures must identify EDE Entity's Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents or Breaches and provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes. EDE Entity agrees to report any Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.

e. Survival. EDE Entity's obligation under this Agreement to protect and maintain the privacy and security of PII and any other obligation of EDE Entity in this Agreement which, by its express terms or nature and context is intended to survive expiration or termination of this Agreement, shall survive the expiration or termination of this Agreement.

f. Severability. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement. In the event that any provision of this Agreement is determined to be invalid, unenforceable or otherwise illegal, such provision shall be deemed restated, in accordance with applicable law, to reflect as nearly as possible the original intention of the Parties, and the remainder of the Agreement shall be in full force and effect.

g. Disclaimer of Joint Venture. Neither this Agreement nor the activities of EDE Entity contemplated by and under this Agreement shall be deemed or construed to create in any way any partnership, joint venture, or agency relationship between CMS and EDE Entity. Neither Party is, nor shall either Party hold itself out to be, vested with any power or right to bind the other Party contractually or to act on behalf of the other Party, except to the extent expressly set forth in the ACA and the regulations codified thereunder, including as codified at 45 C.F.R. part 155.

h. Remedies Cumulative. No remedy herein conferred upon or reserved to CMS under this Agreement is intended to be exclusive of any other remedy or remedies available to CMS under operative law and regulation, and each and every such remedy, to the extent permitted by law, shall be cumulative and in addition to any other remedy now or hereafter existing at law or in equity or otherwise.

i. Records. EDE Entity shall maintain all records that it creates in the normal course of its business in connection with activity under this Agreement for the term of this Agreement in accordance with 45 C.F.R. §§ 155.220(c)(3)(i)(E) or 156.705(c), as applicable. Subject to applicable legal requirements and reasonable policies, such records shall be made available to CMS to ensure compliance with the terms and conditions of this Agreement. The records shall be made available during regular business hours at EDE Entity's offices, and CMS's review shall not interfere unreasonably with EDE Entity's business activities. This clause survives the expiration or termination of this Agreement.

j. Compliance with Law. EDE Entity covenants and agrees to comply with any and all applicable laws, statutes, regulations, or ordinances of the United States of America and any Federal Government agency, board, or court that are applicable to the conduct of the activities that are the subject of this Agreement, including, but not necessarily limited to, any additional and applicable standards required by statute, and any regulations or policies implementing or interpreting such statutory provisions hereafter issued by CMS. In the event of a conflict between the terms of this Agreement and any statutory, regulatory, or sub-regulatory guidance released by CMS, the requirement that constitutes the stricter, higher, or more stringent level of compliance shall control.

k. Governing Law and Consent to Jurisdiction. This Agreement will be governed by the laws and common law of the United States of America, including without limitation such regulations as may be promulgated by HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. EDE Entity further agrees and consents to the jurisdiction of the Federal Courts located within the District of Columbia and the courts of appeal therefrom, and waives any claim of lack of jurisdiction or *forum non conveniens*.

l. Amendment. CMS may amend this Agreement for purposes of reflecting changes in applicable law or regulations, with such amendments taking effect upon thirty (30) Days' written notice to EDE Entity ("CMS notice period"), unless circumstances warrant an earlier effective date. Any amendments made under this provision will only have prospective effect and will not be applied retrospectively. EDE Entity may reject such amendment by providing to CMS, during the CMS notice period, written

notice of its intent to reject the amendment ("rejection notice period"). Any such rejection of an amendment made by CMS shall result in the termination of this Agreement upon expiration of the rejection notice period.

m. Audit and Compliance Review. EDE Entity agrees that CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees may conduct compliance reviews or audits, which includes the right to interview employees, contractors, and business partners of EDE Entity and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of EDE Entity's compliance with the requirements of this Agreement and applicable program requirements upon reasonable notice to EDE Entity, during EDE Entity's regular business hours, and at EDE Entity's regular business location. These audit and review rights include the right to audit EDE Entity's compliance with and implementation of the privacy and security requirements under this Agreement, the ISA, EDE Entity's respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement), and applicable program requirements. EDE Entity further agrees to allow reasonable access to the information and facilities, including, but not limited to, EDE Entity website testing environments, requested by CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees for the purpose of such a compliance review or audit. EDE Entity is also responsible for ensuring cooperation by its Downstream and Delegated Entities, including EDE Entity's subcontractors and assignees, as well as the Auditor(s) and any of its subcontractors, with audits and reviews. CMS may suspend or terminate this Agreement if EDE Entity does not comply with such a compliance review request within seven (7) business days. If any of EDE Entity's obligations under this Agreement are delegated to other parties, the EDE Entity's agreement with any Downstream and Delegated Entities must incorporate this Agreement provision.

   This clause survives the expiration or termination of this Agreement.

n. Access to the FFEs and SBE-FPs. EDE Entity; its Downstream and Delegated Entities, including downstream Agents/Brokers; and its assignees or subcontractors—including, employees, developers, agents, representatives, or contractors—cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to EDE Entity's systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through virtual private networks (VPNs).

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

**This "Agreement between EDE Entity and the Centers for Medicare & Medicaid Services for the Individual Market Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform" has been signed and executed by:**

**TO BE FILLED OUT BY EDE ENTITY**

**The undersigned is an authorized official of EDE Entity who is authorized to represent and bind EDE Entity for purposes of this Agreement. The undersigned attests to the accuracy and completeness of all information provided in this Agreement.**

| | |
|---|---|
| Signature of Authorized Official of EDE Entity | Date |
| Printed Name and Title of Authorized Official of EDE Entity | |
| EDE Entity Name | EDE Entity Partner IDs |
| Signature of Privacy Officer | |
| Printed Name and Title of Privacy Officer | |
| | |
| | |
| EDE Entity Address | |
| EDE Entity Contact Number | |

## FOR CMS

**The undersigned are officials of CMS who are authorized to represent and bind CMS for purposes of this Agreement.**

---

**Jeffrey D. Grant** **Date**
Deputy Director for Operations
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services

---

**George C. Hoffmann** **Date**
Deputy CIO and Deputy Director
Office of Information Technology (OIT)
Centers for Medicare & Medicaid Services (CMS)

## APPENDIX A: PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS FOR NON-EXCHANGE ENTITIES

Federally-facilitated Exchanges ("FFEs") will enter into contractual agreements with all Non-Exchange Entities, including EDE Entities, that gain access to Personally Identifiable Information ("PII") exchanged with the FFEs (including FF-SHOPs) and State-based Exchanges on the Federal Platform ("SBE-FPs") (including SBE-FP-SHOPs), or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representatives or Authorized Representatives. This Agreement and its appendices govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by EDE Entities in the context of the FFEs and SBE-FPs. In signing this contractual Agreement, in which this Appendix A has been incorporated, EDE Entities agree to comply with the security and privacy standards and implementation specifications outlined in the Non-Exchange Entity System Security and Privacy Plan ("NEE SSP")[30] and Section A[31] below while performing the Authorized Functions outlined in their respective Agreement(s) with CMS.

The standards documented in the NEE SSP and Section A below are established in accordance with Section 1411(g) of the Affordable Care Act ("ACA") (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 ("FISMA") (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the principles in 45 C.F.R. §§ 155.260(a)(1) through (a)(6). All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

### A. NON-EXCHANGE ENTITY PRIVACY AND SECURITY IMPLEMENTATION SPECIFICATIONS

Non-Exchange Entities must meet privacy and security implementation specifications that are consistent with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 P.L. 104-191 and the Privacy Act of 1974, 5 U.S.C. § 552a, including:

(1) Openness and Transparency. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, and Enrollees and their PII.

a. Standard: Privacy Notice Statement. Prior to collecting PII, the Non-Exchange Entity must provide a notice that is prominently and conspicuously displayed on a public-facing website, if applicable, or on the electronic and/or paper form the

[30] The NEE SSP template is located on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

[31] Section A contains excerpts from the NEE SSP of two requirements for ease of reference. This does not alter the need to comply with other applicable EDE Entity requirements, including those outlined within 45 C.F.R. § 155.260(a)(1) through (a)(6) or the NEE SSP.

Non-Exchange Entity will use to gather and/or request PII. The EDE Entity must comply with any additional standards and implementation specifications described in NEE SSP TR-1: Privacy Notice.

i. Implementation Specifications.

1. The statement must be written in plain language and provided in a manner that is timely and accessible to people living with disabilities and with limited English proficiency.

2. The statement must contain at a minimum the following information:

a. Legal authority to collect PII;

b. Purpose of the information collection;

c. To whom PII might be disclosed, and for what purposes;

d. Authorized uses and disclosures of any collected information;

e. Whether the request to collect PII is voluntary or mandatory under the applicable law; and

f. Effects of non-disclosure if an individual chooses not to provide the requested information.

3. The Non-Exchange Entity shall maintain its Privacy Notice Statement content by reviewing and revising as necessary on an annual basis, at a minimum, and before or as soon as possible after any change to its privacy policies and procedures.

4. If the Non-Exchange Entity operates a website, it shall ensure that descriptions of its privacy and security practices, and information on how to file complaints with CMS and the Non-Exchange Entity, are publicly available through its website.[32]

(2) Individual Choice. In keeping with the standards and implementation specifications used by the FFEs, the Non-Exchange Entity should ensure that Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—are provided a reasonable opportunity and capability to make informed decisions about the creation, collection, disclosure, access, maintenance, storage, and use of their PII.

a. Standard: Informed Consent. The Non-Exchange Entity may create, collect, disclose, access, maintain, store, and use PII from Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—only for the functions and purposes listed in the

[32] CMS recommends that EDE Entities direct consumers, who are seeking to file a complaint, to the Secretary of the U.S. Department of Health and Human Services, 200 Independence Ave, S.W., Washington, D.C. 20201. Call (202) 619-0257 (or toll free (877) 696-6775) or go to the website of the Office for Civil Rights, www.hhs.gov/ocr/hipaa.

Privacy Notice Statement and any relevant agreements in effect as of the time the information is collected, unless the FFE, SBE-FP, or Non-Exchange Entity obtains informed consent from such individuals. The EDE Entity must comply with any additional standards and implementation specifications described in NEE SSP IP-1: Consent.

i. Implementation Specifications.

1. The Non-Exchange Entity must obtain informed consent from individuals for any use or disclosure of information that is not permissible within the scope of the Privacy Notice Statement and any relevant agreements that were in effect as of the time the PII was collected. Such consent must be subject to a right of revocation.

2. Any such consent that serves as the basis of a use or disclosure must:

    a. Be provided in specific terms and in plain language,

    b. Identify the entity collecting or using the PII, and/or making the disclosure,

    c. Identify the specific collections, use(s), and disclosure(s) of specified PII with respect to a specific recipient(s), and

    d. Provide notice of an individual's ability to revoke the consent at any time.

3. Consent documents must be appropriately secured and retained for ten (10) Years.

## APPENDIX B: DEFINITIONS

This Appendix defines terms that are used in the Agreement and other Appendices. Any capitalized term used in the Agreement that is not defined therein or in this Appendix has the meaning provided in 45 C.F.R. § 155.20.

(1) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 C.F.R. § 155.20.

(2) **Affordable Care Act (ACA)** means the Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), which are referred to collectively as the Affordable Care Act or ACA.

(3) **Agent** or **Broker** has the meaning set forth in 45 C.F.R. § 155.20.

(4) **Agent or Broker Direct Enrollment (DE) Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.

(5) **Applicant** has the meaning set forth in 45 C.F.R. § 155.20.

(6) **Auditor** means a person or organization that meets the requirements set forth in this Agreement and contracts with a Direct Enrollment (DE) Entity for the purposes of conducting an Operational Readiness Review (ORR) in accordance with 45 C.F.R. §§ 155.221(b)(4) and (f), this Agreement and CMS-issued guidance.

(7) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in the Agreement that incorporates this Appendix B.

(8) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 C.F.R. § 155.227.

(9) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information for anything other than an authorized purpose.

(10) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (CMS).

(11) **Classic Direct Enrollment (Classic DE)** means, for purposes of this Agreement, the original version of Direct Enrollment, which utilizes a double redirect from a Direct Enrollment (DE) Entity's website to HealthCare.gov where the eligibility application is submitted and an eligibility determination is received, and back to the DE Entity's

website for QHP shopping and plan selection consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(i), 155.221, 156.265 and/or 156.1230(b).

(12) **Classic Direct Enrollment Pathway (Classic DE Pathway)** means, for the purposes of this Agreement, the application and enrollment process used by Direct Enrollment (DE) Entities for Classic DE.

(13) **CMS** means the Centers for Medicare & Medicaid Services.

(14) **CMS Companion Guides** means a CMS-authored guide, available on the CMS website, which is meant to be used in conjunction with and supplement relevant implementation guides published by the Accredited Standards Committee.

(15) **CMS Data Services Hub (Hub)** is the CMS Federally-managed service to interface data among connecting entities, including HHS, certain other Federal agencies, and State Medicaid agencies.

(16) **CMS Data Services Hub Web Services (Hub Web Services)** means business and technical services made available by CMS to enable the determination of certain eligibility and enrollment or federal financial payment data through the Federally-facilitated Exchange (FFE) website, including the collection of personal and financial information necessary for Consumer, Applicant, Qualified Individual, or Enrollee account creations; Qualified Health Plan (QHP) application submissions; and Insurance Affordability Program eligibility determinations.

(17) **Common Control** means a security or privacy control whose implementation results in a security or privacy capability that is inheritable by multiple information systems being served by the Primary EDE Entity.

(18) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (QHP) offered through an Exchange or Insurance Affordability Program, or whom an Agent or Broker (including Web-brokers) registered with the FFE, Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a QHP, applying for APTC and CSRs, and/or completing enrollment in a QHP through the FFEs or State-based Exchanges on the Federal Platform (SBE-FPs) for individual market coverage.

(19) **Cost-sharing Reductions (CSRs)** has the meaning set forth in 45 C.F.R. § 155.20.

(20) **Customer Service** means assistance regarding eligibility and Health Insurance Coverage provided to a Consumer, Applicant, Qualified Individual, and Enrollee, including, but not limited to, responding to questions and complaints; providing information about eligibility; applying for APTC and/or CSRs, and Health Insurance Coverage; and explaining enrollment processes in connection with the FFEs or SBE-FPs.

(21) **Day or Days** means calendar days, unless otherwise expressly indicated in the relevant provision of the Agreement that incorporates this Appendix B.

(22) **Delegated Entity** means, for purposes of this Agreement, any party, including an Agent or Broker, that enters into an agreement with an Enhanced Direct Enrollment (EDE Entity) to provide administrative or other services to or on behalf of the EDE Entity or to provide administrative or other services to Consumers and their dependents.

(23) **Designated Privacy Official** means a contact person or office responsible for receiving complaints related to Breaches or Incidents, able to provide further information about matters covered by the Privacy Notice statement, responsible for the development and implementation of the privacy policies and procedures of the Non-Exchange Entity, and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy of Personally Identifiable Information (PII).

(24) **Designated Representative** means an Agent or Broker that has the legal authority to act on behalf of the Web-broker.

(25) **Designated Security Official** means a contact person or office responsible for the development and implementation of the security policies and procedures of the Non-Exchange Entity and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the security of Personally Identifiable Information (PII).

(26) **Direct Enrollment (DE)** means, for the purposes of this Agreement, the process by which a Direct Enrollment (DE) Entity may assist an Applicant or Enrollee with enrolling in a QHP in a manner that is considered through the Exchange consistent with applicable requirements in 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or 156.1230. Direct Enrollment is the collective term used when referring to both Classic Direct Enrollment and Enhanced Direct Enrollment.

(27) **Direct Enrollment (DE) Entity** has the meaning set forth in 45 C.F.R. § 155.20.

(28) **Direct Enrollment Entity Application Assister** has the meaning set forth in 45 C.F.R. § 155.20.

(29) **Direct Enrollment (DE) Environment** means an information technology application or platform provided, owned, and maintained by a DE Entity through which a DE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.

(30) **Downstream Entity** means, for purposes of this Agreement, any party, including an Agent or Broker, that enters into an agreement with a Delegated Entity or with another Downstream Entity for purposes of providing administrative or other services related to the agreement between the Delegated Entity and the Enhanced Direct Enrollment (EDE) Entity. The term "Downstream Entity" is intended to refer to the

entity that directly provides administrative services or other services to or on behalf of the EDE Entity or that provides administrative or other services to Consumers and their dependents.

(31) **Downstream White-Label Third-Party User Arrangements** means an arrangement between an Agent or Broker and a Primary EDE Entity to use the Primary EDE Entity's EDE Environment. In this arrangement, a Primary EDE Entity enables the Downstream White-Label Agent or Broker to only make minor branding changes to the Primary EDE Entity's EDE Environment.

(32) **Enhanced Direct Enrollment (EDE)** means, for purposes of this Agreement, the version of Direct Enrollment which allows Consumers, Applicants, Qualified Individuals, or Enrollees—or these individuals' legal representatives or Authorized Representatives—to complete all steps in the application, eligibility and enrollment processes on an EDE Entity's website consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(ii), 155.221, 156.265 and/or 156.1230(b) using application programming interfaces (APIs) as provided, owned, and maintained by CMS to transfer data between the Exchange and the EDE Entity's website.

(33) **Enhanced Direct Enrollment (EDE) End-User Experience** means all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions under this Agreement.

(34) **Enhanced Direct Enrollment (EDE) Entity** means a DE Entity that has been approved by CMS to use the EDE Pathway. This term includes both Primary EDE Entities and Upstream EDE Entities.

(35) **Enhanced Direct Enrollment (EDE) Environment** means an information technology application or platform provided, owned, and maintained by an EDE Entity through which an EDE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee—or these individuals' legal representatives or Authorized Representatives—information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.

(36) **Enhanced Direct Enrollment (EDE) Pathway** means the APIs and functionality comprising the systems that enable EDE as provided, owned, and maintained by CMS.

(37) **Enrollee** has the meaning set forth in 45 C.F.R. § 155.20.

(38) **Exchange** has the meaning set forth in 45 C.F.R. § 155.20.

(39) **Federally-facilitated Exchange (FFE)** means an **Exchange** (or **Marketplace**) established by the Department of Health and Human Services (HHS) and operated by

CMS under Section 1321(c)(1) of the ACA for individual market coverage. **Federally-facilitated Marketplaces (FFMs)** has the same meaning as FFEs.

(40) **Health Insurance Coverage** has the meaning set forth in 45 C.F.R. § 155.20.

(41) **Health Insurance Portability and Accountability Act (HIPAA)** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and its implementing regulations.

(42) **Health Reimbursement Arrangement (HRA)** has the meaning set forth in 45 C.F.R. § 146.123(c).

(43) **HHS** means the United States Department of Health & Human Services.

(44) **Hybrid Control** means those controls for which both a Primary EDE Entity and its Upstream EDE Entity share the responsibility of implementing the full control objectives and implementation standards. Hybrid Controls refer to arrangements in which an Upstream EDE Entity information system inherits part of a control from a Primary EDE Entity, with the remainder of the control provided by the Upstream EDE Entity leveraging the Primary EDE Entity's EDE Environment.

(45) **Hybrid Issuer Upstream EDE Entity** means a QHP Issuer EDE Entity that uses the EDE Environment of a Primary EDE Entity and adds functionality or systems to the Primary EDE Entity's EDE Environment such that the Primary EDE Entity's EDE Environment or overall EDE End-User Experience is modified beyond minor deviations for branding or QHP display changes relevant to the Issuer's QHPs.

(46) **Hybrid Non-Issuer Upstream EDE Entity** means an Agent, Broker, or Web-broker under 45 C.F.R. §§ 155.220(c)(3) and 155.221 that uses the EDE Environment of a Primary EDE Entity and adds functionality or systems to the Primary EDE Entity's EDE Environment such that the Primary EDE Entity's EDE Environment or overall EDE End-User Experience is modified beyond minor branding changes.

(47) **Incident**, or **Security Incident**, has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and means an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

(48) **Insurance Affordability Program** means a program that is one of the following:

(1) A State Medicaid program under title XIX of the Social Security Act.

(2) A State Children's Health Insurance Program (CHIP) under title XXI of the Social Security Act.

(3) A State basic health program established under section 1331 of the Care Act.

(4) A program that makes coverage in a Qualified Health Plan (QHP) through the Exchange with APTC established under section 36B of the Internal Revenue Code available to Qualified Individuals.

(5) A program that makes available coverage in a QHP through the Exchange with CSRs established under section 1402 of the ACA.

(49) **Interconnection Security Agreement** means a distinct agreement that outlines the technical solution and security requirements for an interconnection between CMS and EDE Entity.

(50) **Issuer** has the meaning set forth in 45 C.F.R. § 144.103.

(51) **Non-Exchange Entity** has the meaning at 45 C.F.R. § 155.260(b)(1), including, but not limited to, Qualified Health Plan (QHP) Issuers, Navigators, Agents, Brokers, and Web-brokers.

(52) **OMB** means the Office of Management and Budget.

(53) **Operational Readiness Review (ORR)** means an audit conducted under 45 C.F.R. §§ 155.221(b)(4) and (f) and includes the reports submitted by an EDE Entity detailing its compliance with CMS requirements and readiness to implement and use the EDE Environment.

(54) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

(55) **Primary EDE Entity** means an entity that has developed and maintains an EDE Environment. A Primary EDE Entity may provide its EDE Environment to an Upstream EDE Entity and the Primary EDE Entity may provide an EDE Environment for use by Consumers, Applicants, Qualified Individuals, Enrollees—or these individuals' legal representatives or Authorized Representatives—, Agents, Brokers, or DE Entity Application Assisters.

(56) **Prospective EDE Entity** means an entity that has not yet been approved by CMS to use the EDE Pathway.

(57) **Prospective Phase Change EDE Entity** means a Primary EDE Entity already approved to use the EDE Pathway that is seeking to implement a new eligibility application phase using the EDE Entity-initiated Change Request process.

(58) **Qualified Health Plan (QHP)** has the meaning set forth in 45 C.F.R. § 155.20.

(59) **Qualified Health Plan (QHP) Issuer** has the meaning set forth in 45 C.F.R. § 155.20.

(60) **Qualified Health Plan (QHP) Issuer Agreement** means the QHP Certification Agreement and Privacy and Security Agreement Between QHP Issuer and CMS.

(61) **Qualified Health Plan (QHP) Direct Enrollment (DE) Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.

(62) **Qualified Individual** has the meaning set forth in 45 C.F.R. § 155.20.

(63) **Rules of Engagement (ROE)** means the detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test and gives the test team authority to conduct defined activities without the need for additional permissions.

(64) **Special Enrollment Period (SEP)** has the meaning set forth in 45 C.F.R. § 155.20.

(65) **Standalone Eligibility Service (SES)** means a suite of application program interfaces (APIs) that will allow an EDE Entity to create, update, submit, and ultimately retrieve eligibility results for an application.

(66) **State** means the State that has licensed the Agent, Broker, Web-broker, or Issuer that is a party to this Agreement and in which the Agent, Broker, Web-broker, or Issuer is operating.

(67) **State-based Exchange (SBE)** means an Exchange established by a State that receives approval to operate under 45 C.F.R. § 155.105. **State-based Marketplace ("SBM")** has the same meaning as SBE.

(68) **State-based Exchange on the Federal Platform (SBE-FP)** means an Exchange established by a State that receives approval under 45 C.F.R. § 155.106(c) to utilize the Federal platform to support select eligibility and enrollment functions. **State-based Marketplace on the Federal Platform ("SBM-FP")** has the same meaning as SBE-FP.

(69) **Streamlined Eligibility Application User Interface (UI)** means the application UI on HealthCare.gov available for Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—with non-complex eligibility application responses determined by an initial set of eligibility questions for determining the complexity of an Applicant's eligibility profile.

(70) **Upstream EDE Entity** means an EDE Entity that uses the EDE Environment of a Primary EDE Entity and meets the definition of a Hybrid Issuer Upstream EDE Entity; a Hybrid Non-Issuer Upstream EDE Entity; or a White-Label Issuer Upstream EDE Entity.

(71) **Web-broker** has the meaning set forth in 45 C.F.R. § 155.20.

(72) **Web-broker Agreement** means the Agreement between a Web-broker and CMS for the FFEs and SBE-FPs.

(73) **White-Label Issuer Upstream EDE Entity** means a QHP Issuer that uses the EDE Environment of a Primary EDE Entity without modifications beyond minor branding changes or QHP display changes.

(74) **Workforce** means a Non-Exchange Entity's employees, contractors, subcontractors, officers, directors, agents, representatives, and any other individual who may create, collect, disclose, access, maintain, store, or use PII in the performance of his or her duties.

## APPENDIX C: EDE BUSINESS REQUIREMENTS[33]

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

| Review Category | Requirement and Audit Standard |
|---|---|
| **Consumer Identity Proofing Implementation** | ▪ *Requirement*: The EDE Entity must conduct identity proofing (ID proofing) for Consumers entering the EDE pathway for enrollments through both Consumer and in-person Agent and Broker pathways.[34] The EDE Entity must conduct ID proofing prior to submitting a Consumer's application to the Exchange. If an EDE Entity is unable to complete ID proofing of the Consumer, the EDE Entity may either direct the Consumer to the classic DE (i.e., double-redirect) pathway or direct the Consumer to the Exchange (HealthCare.gov or the Exchange Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]).<br>– Remote ID Proofing/Fraud Solutions Archive Reporting Services (RIDP/FARS) or Third-Party ID Proofing Service: CMS will make the Exchange RIDP and FARS services available for the EDE Entity to use when remote ID proofing Consumers for the Consumer pathway (i.e., when a Consumer is interacting directly with the EDE environment without the assistance of an individual Agent or Broker). If an EDE Entity uses the Exchange RIDP service, it must use the RIDP service only after confirming the Consumer is seeking coverage in a State supported by the Exchange/Federal Platform, and only after confirming the Consumer is eligible for the EDE Entity's chosen phase. However, CMS does not require that EDE Entities use the Exchange RIDP and FARS services, specifically, to complete ID proofing. An EDE Entity may instead opt to use a third-party ID proofing service for ID proofing in the Consumer pathway. If an EDE Entity uses a third-party identity proofing service, the service must be Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS)-approved, and the EDE Entity must be able to produce documentary evidence that each Applicant has been successfully ID proofed. Documentation related to a third-party service could be requested in an audit or investigation by CMS (or its designee), pursuant to the EDE Business Agreement. Applicants do not need to be ID proofed on subsequent interactions with the EDE Entity if the Applicant creates an account (i.e., username and password) on the EDE Entity's website, and the EDE Entity tracks that ID proofing has occurred when the Applicant's account was created.<br>– Manual ID Proofing in the In-Person Agent and Broker Pathway: EDE Entities may also offer a manual ID proofing process. Consumers being ID proofed in the in-person Agent and Broker pathway (i.e., when an Agent or Broker is working with a Consumer and conducting ID proofing in-person, rather than remotely) must be ID proofed following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE (https://zone.cms.gov/document/api-information). |

[33] The table in Appendix C is an updated version of Exhibit 2 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

[34] Consumer pathway means the workflow, UI, and accompanying APIs for an EDE environment that is intended for use by a Consumer to complete an eligibility application and enrollment. Agent and Broker pathway means the workflow, UI, and accompanying APIs for an EDE environment that is intended for use by an Agent or Broker to assist a Consumer with completing an eligibility application and enrollment.

| Review Category | Requirement and Audit Standard |
|---|---|
| **Consumer Identity Proofing Implementation (continued)** | – For the Consumer pathway, the EDE Entity must provide the User ID of the requester in the header for each EDE API call. For the Consumer pathway, the User ID should be the User ID for the Consumer's account on the EDE Entity's site, or some other distinct identifier the EDE Entity assigns to the Consumer.<br>– Additionally, if an EDE Entity is using the Fetch Eligibility API, the same User ID requirements apply. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID.<br>▪ Review Standard:<br>– If an EDE Entity uses the Exchange RIDP service, the Auditor must verify that the EDE Entity has successfully passed testing with the Hub..[35]<br>– If an EDE Entity uses a third-party ID proofing service, the Auditor must evaluate and certify the following:<br>The ID proofing service is FICAM TFS-approved, and<br>The EDE Entity has implemented the service correctly.<br>– If an EDE Entity offers a Manual ID proofing option for an in-person Agent and Broker pathway, the Auditor must verify that the EDE Entity requires Agents and Brokers to ID proof Consumers as described in the "Acceptable Documentation for Identity Proofing" document.<br>– EDE Entity's inclusion of the appropriate Consumer User ID fields in the EDE and Fetch Eligibility API calls. |

[35] RIDP/FARS testing requirements for the Hub can be found at the following link on CMS zONE: https://zone.cms.gov/document/api-information.

| Review Category | Requirement and Audit Standard |
|---|---|
| **Agent and Broker Identity Proofing Verification** | ▪ *Requirement:* If an EDE Entity is implementing an Agent and Broker pathway for its EDE environment, the EDE Entity must implement Agent and Broker ID proofing verification procedures that consist of the following requirements:<br>– EDE Entity must integrate with IDM-Okta[36] and provide the User ID of the requester and IDM-Okta token in the header for each EDE API call. For Agents and Brokers, the User ID must exactly match the Exchange User ID (i.e. the Agent's or Broker's portal.cms.gov User ID) for the Agent or Broker, or the request will fail Exchange User ID validation. The same User ID requirements apply to the Fetch Eligibility and Submit Enrollment APIs. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID.<br>– EDE Entity must ID proof all Agents and Brokers prior to allowing the Agents and Brokers to use its EDE environment. EDE Entity may conduct ID proofing in one of the following ways:<br>Use the Exchange-provided RIDP/FARS APIs to remotely ID proof Agents and Brokers; OR<br>Manually ID proof Agents and Brokers following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE EDE webpage (https://zone.cms.gov/document/api-information). EDE Entities are permitted to use manual ID proofing as an alternative for Agents and Brokers that cannot be ID proofed via the RIDP/FARS services.<br>– EDE Entity must validate an Agent's or Broker's National Producer Number (NPN) using the National Insurance Producer Registry (https://www.nipr.com) prior to allowing the Agent or Broker to use its EDE environment.<br>– EDE Entity must systematically provide an Agent and Broker ID proofing process—that meets all of the requirements defined here—that applies to all downstream Agents and Brokers of the Primary EDE Entity.<br>– Additionally, all Agent and Broker users of an Upstream EDE Entity's EDE website (hosted by a Primary EDE Entity) must be ID proofed consistent with these requirements. The Primary EDE Entity may provide one centralized ID proofing approach for any Agents and Brokers that will use the Primary EDE Entity's EDE environment (including when utilized by Upstream EDE Entities and their downstream Agents and Brokers). |

[36] For instructions on how to integrate with IDM-Okta, see the Change Request #55 Integration Manual (IDM Integration), available at: https://zone.cms.gov/document/business-audit and *Hub Onboarding Form*, available at: https://zone.cms.gov/document/hub-onboarding-form.

| Review Category | Requirement and Audit Standard |
|---|---|
| **Agent and Broker Identity Proofing Verification (continued)** | Alternatively, the Upstream EDE Entity may conduct its own ID proofing process of its downstream Agents and Brokers consistent with these requirements. The Upstream EDE Entity must provide the information for Agents and Brokers that have passed and failed ID proofing to the Primary EDE Entity using a secure data transfer. If an Upstream EDE Entity wants to pursue this flexibility, its ID proofing process must be audited by an Auditor consistent with these standards and the arrangement will be considered a hybrid arrangement.<br>– Note: If a Primary EDE Entity does not provide a centralized process for ID proofing an Upstream EDE Entity's downstream Agent and Broker and if the Primary EDE Entity intends to provide the EDE environment to Upstream EDE Entities, the Upstream EDE Entities will be required to provide documentation of an Auditor's evaluation of its ID proofing approach consistent with these standards. This process must be categorized as an EDE Entity-initiated Change Request (Section XI.A, EDE Entity-initiated Change Requests) if it occurs after the Primary EDE Entity's initial audit submission and the arrangement with the Upstream EDE Entity will be considered a hybrid arrangement.<br>– All Agents and Brokers that will use EDE must be ID proofed consistent with these standards. This includes downstream Agents and Brokers of Primary EDE Entities and Upstream EDE Entities. If applicable, the Auditor must evaluate the Primary EDE Entity's centralized implementation for ID proofing or the Upstream EDE Entity's implementation for ID proofing.<br>– EDE Entity is strongly encouraged to implement multi-factor authentication for Agents and Brokers that is consistent with NIST SP 800-63-3.<br>▪ *Review Standard:* The Auditor must verify and certify the following:<br>– EDE Entity's inclusion of the appropriate Agent and Broker User ID and IDM-Okta token fields in the EDE and Fetch Eligibility and Submit Enrollment API calls.<br>– EDE Entity's process for ID proofing an Agent or Broker prior to allowing an Agent or Broker to use its EDE environment.<br>– EDE Entity's process for validating an Agent's or Broker's NPN using the National Insurance Producer Registry prior to allowing an Agent or Broker to use its EDE environment.<br>– EDE Entity's process for systematically providing an Agent and Broker ID proofing approach for all downstream Agents and Brokers of the EDE Entity and, if applicable, any Upstream EDE Entities.<br>– If the Primary EDE Entity has not provided a centralized ID proofing approach to an Upstream EDE Entity, Primary EDE Entity's process for verifying that an Upstream EDE Entity has conducted appropriate ID proofing, consistent with this requirement, for all of the Upstream EDE Entity's downstream Agents and Brokers prior to those Agents and Brokers being able to use the Primary EDE Entity's EDE environment. |
| **Phase-dependent Screener Questions (EDE Phase 1 and 2 EDE Entities Only)** | ▪ *Requirement:* An EDE Entity that implements either EDE Phase 1 or Phase 2 must implement screening questions to identify Consumers whose eligibility circumstances the EDE Entity is unable to support consistent with the eligibility scenarios supported by the EDE Entity's selected EDE phase. These phase-dependent screener questions must be located at the beginning of the EDE application, but may follow the QHP plan compare experience. For those Consumers who won't be able to apply through scenarios covered by the EDE phase that the EDE Entity implements, the EDE Entity must either route the Consumer to the classic DE double-redirect pathway or direct the Consumer to the Exchange by providing the following options: HealthCare.gov or the Exchange Call Center at 1-800-318-2596 [TTY: 1-855-889-4325].<br>▪ *Review Standard*: The Auditor must verify the following:<br>– The EDE Entity has implemented screening questions—consistent with the requirements in the Exchange Application UI Principles document and Application UI Toolkit—to identify Consumers with eligibility scenarios not supported by the EDE Entity's EDE environment and selected EDE phase.<br>– The EDE Entity's EDE environment facilitates moving Consumers to one of the alternative enrollment pathways described immediately above. |

| Review Category | Requirement and Audit Standard |
|---|---|
| **Accurate and Streamlined Eligibility Application User Interface (UI)** | *Requirement:* EDE Entities using the EDE pathway must support all application scenarios outlined in EDE Entity's selected EDE phase. The EDE Entity must adhere to the guidelines set forth in the FFE Application UI Principles document when implementing the application. EDE Entities can access the FFE Application UI Principles document on CMS zONE (https://zone.cms.gov/document/eligibility-information). Auditors will need to access the FFE Application UI Principles document to conduct the audit.<br>– As explained in the FFE Application UI Principles document, the EDE Entity must implement the application in accordance with the Exchange requirements. For each supported eligibility scenario, the EDE Entity must display all appropriate eligibility questions and answers, including all questions designated as optional. (Note: These questions are optional for the Consumer to answer, but are not optional for EDE Entities to implement.) The FFE Application UI Principles document and Application UI Toolkit define appropriate flexibility EDE Entities may implement with respect to question wording, question order or structure, format of answer choices (e.g., drop-down lists, radio buttons), and integrated help information (e.g., tool tips, URLs, help boxes). In most cases, answer choices, question logic (e.g., connections between related questions), and disclaimers (e.g., APTC attestation) must be identical to those of the Exchange.<br>Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this exceeds the scope of the test cases in the Eligibility Results Toolkits.<br>– EDE Entities will also need to plan their application's back-end data structure to ensure that attestations can be successfully submitted to Standalone Eligibility Service (SES) APIs at appropriate intervals within the application process and that the EDE Entity can process responses from SES and integrate them into the UI question flow logic, which is dynamic for an individual Consumer based on his or her responses. The EDE Entity will need to ensure that sufficient, non-contradictory information is collected and stored such that accurate eligibility results will be reached without any validation errors.<br>▪ *Review Standard*: The Auditor must review and certify the following:<br>– The FFE Application UI has been implemented in EDE Entity's environment in accordance with the Exchange Application UI Principles document.<br>– The FFE Application UI displays all appropriate eligibility questions and answers from the Application UI Toolkit, including any questions designated as optional.<br>– The Auditor will review the application for each supported eligibility scenario under the phase the EDE Entity has implemented to confirm that the application has been implemented in accordance with the FFE Application UI Principles document and Application UI Toolkit. The Auditor will document this compliance in the Application UI Toolkit.<br>Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this exceeds the scope of the test cases in the Eligibility Results Toolkits.<br>– If EDE Entity has implemented Phase 1 or Phase 2, the Auditor will confirm that the UI includes a disclaimer stating that the environment does not support all application scenarios, and identifying which scenarios are and are not supported. The disclaimer should direct the Consumer to alternative pathways, such as the classic DE double-redirect pathway or direct the Consumer to the Exchange (HealthCare.gov or the Exchange Call Center at 1-800-318-2596 (TTY: 1-855-889-4325)). This requirement is included in the Communications Toolkit. |

| Review Category | Requirement and Audit Standard |
|---|---|
| **Post-eligibility Application Communications** | ▪ *Requirement*: The EDE environment must display high-level eligibility results, next steps for enrollment, and information about each Applicant's insurance affordability program eligibility (e.g., APTC, CSR, Medicaid, and/or CHIP eligibility), Data Matching Issues (DMIs), special enrollment periods (SEPs), SEP Verification Issues (SVIs), and enrollment steps in a clear, comprehensive and Consumer-friendly way. Generally, CMS's Communications Toolkit constitutes the minimum post-eligibility application communications requirements that an EDE Entity must provide to users of the EDE environment; CMS does not intend for the Communications Toolkit requirements to imply that EDE Entities are prohibited from providing additional communications or functionality, consistent with applicable requirements.<br>– EDE Entity must provide Consumers with required UI messaging tied to API functionality and responses as provided in the EDE API Companion Guide[37].<br>– EDE Entity must provide Consumers with the CMS-provided Eligibility Determination Notices (EDNs) generated by the Exchange any time it submits or updates an application pursuant to requirements provided by CMS in the Communications Toolkit. |

[37] The API Companion Guide is available on CMS zONE at the following link: https://zone.cms.gov/document/api-information.

| Review Category | Requirement and Audit Standard |
|---|---|
| **Post-eligibility Application Communications (continued)** | – EDE Entity must provide the EDN in a downloadable format at the time the Consumer's application is submitted or updated and must have a process for providing access to the Consumer's most recent EDN via the API as well as providing access to the Consumer's historical notices—accessed via the Notice Retrieval API by the EDE Entity's EDE environment—within the UI. The UI requirements related to accessibility of a Consumer's EDN are set forth in the Communications Toolkit.<br>– EDE Entities are not required to store notices downloaded from the Exchange. EDE Entities must use the Metadata Search API and the Notice Retrieval API to generate the most recent Exchange notices when Consumers act to view/download notices consistent with the Communications Toolkit. EDE Entities must also provide access to view/download historical notices in their UIs.<br>– EDE Entity must provide and communicate status updates and access to information for Consumers to manage their applications and coverage. These communications include, but are not limited to, status of DMIs and SVIs, enrollment periods (e.g., SEP eligibility and the OEP), providing and communicating about new notices generated by the Exchange, application and enrollment status, and supporting document upload for DMIs and SVIs. This requirement is detailed in the Communications Toolkit.<br>– EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI (e.g., an account management hub for managing all application- and enrollment-related actions).<br>– For any Consumers enrolled, including via the Agent and Broker pathway, the EDE Entity must provide critical communications to Consumers notifying them of the availability of Exchange-generated EDNs, critical communications that the Consumer will no longer receive from the Exchange (i.e., if the EDE Entity has implemented and been approved by CMS to assume responsibility for those communications), and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer's application or enrollment status.<br>– All EDE Entities, regardless of phase, must provide Consumers with status updates and document upload capabilities for all DMIs and SVIs. Even if an EDE Entity's chosen eligibility application phase does not support the questions necessary to reach a certain DMI or SVI, the post-application and post-enrollment functionality must support any Consumer with any DMI or SVI; post-application and post-enrollment DMI and SVI management is not dependent on the EDE Entity's chosen eligibility application phase.<br>▪ *Review Standard*: The Auditor must verify and certify the following:<br>– The EDE Entity's EDE environment is compliant with the requirements contained in the Communications Toolkit and API Companion Guide.<br>– The EDE Entity's EDE environment notifies Consumers of their eligibility results prior to QHP enrollment, including when submitting a CiC in the environment. For example, if a Consumer's APTC or CSR eligibility changes, EDE Entity must notify the Consumer of the change and allow the Consumer to modify his or her QHP selection (if SEP-eligible) or APTC allocation accordingly.<br>– EDE Entity must have a process for providing Consumers with a downloadable EDN in its EDE environment and for providing access to a current EDN via the API. EDE Entity must share required eligibility information that is specified by CMS in the Communications Toolkit.<br>– The Auditor must verify that EDE Entity's EDE environment is providing status updates and ongoing communications to Consumers according to CMS requirements in the Communications Toolkit as it relates to the status of their application, eligibility, enrollment, notices, and action items the Consumer needs to take.<br>– The EDE Entity must provide application and enrollment management functions for the Consumer in a clear, accessible location in the UI.<br>– The EDE Entity must have a means for providing critical communications to the Consumer consistent with the standards above.<br>– The EDE Entity must support all DMIs and SVIs in its post-eligibility application and post-enrollment functionality. |

| Review Category | Requirement and Audit Standard |
|---|---|
| **Accurate Information about the Exchange and Consumer Communications** | ▪ *Requirement:* EDE Entity must provide Consumers with CMS-provided language informing and educating the Consumers about the Exchanges and HealthCare.gov and Exchange-branded communications Consumers may receive with important action items. CMS defines these requirements in the Communications Toolkit.<br>▪ *Review Standard:* The Auditor must verify and certify that the EDE Entity's EDE environment includes all required language, content, and disclaimers provided by CMS in accordance with the standards stated in guidance and the Communications Toolkit. |
| **Documentation of Interactions with Consumer Applications or the Exchange** | ▪ *Requirement:* EDE Entity must implement and maintain tracking functionality on its EDE environment to track Agent, Broker, and Consumer interactions, as applicable, with Consumer applications using a unique identifier for each individual, as well as an individual's interactions with the Exchanges (e.g., application; enrollment; and handling of action items, such as uploading documents to resolve a DMI). This requirement also applies to any actions taken by a downstream Agent or Broker,[38] as well as the Upstream EDE Entity users, of a Primary EDE Entity's EDE environment.<br>▪ *Review Standard:* The Auditor must verify EDE Entity's process for determining and tracking when an Upstream EDE Entity, downstream Agent or Broker, and Consumer has interacted with a Consumer application or taken actions utilizing the EDE environment or EDE APIs. The Auditor must verify and certify the following:<br>– The EDE Entity's environment tracks, at a minimum, the interactions of Upstream EDE Entities, downstream Agents or Brokers, and Consumers with a Consumer's account, records, application, or enrollment information utilizing the EDE environment or EDE APIs.<br>– The EDE Entity's environment tracks when an upstream Entity, downstream Agent or Broker, or Consumer views a Consumer's record, enrollment information, or application information utilizing the EDE environment or EDE APIs.<br>– The EDE Entity's environment uses unique identifiers to track and document activities by Consumers, downstream Agents and Brokers, and Upstream EDE Entities using the EDE environment.<br>– The EDE Entity's environment tracks interactions with the EDE suite of APIs by an Upstream EDE Entity, a downstream Agent or Broker, or Consumer.<br>– The EDE Entity's environment stores this information for 10 years. |

[38] Note: References to downstream Agents and Brokers include downstream Agents and Brokers of either the Primary EDE Entity or an Upstream EDE Entity.

| Review Category | Requirement and Audit Standard |
|---|---|
| **Eligibility Results Testing and SES Testing** | ▪ *Requirement*: EDE Entity must submit accurate applications through its EDE environment that result in accurate and consistent eligibility determinations for the supported eligibility scenarios covered by EDE Entity's chosen EDE phase.<br>– The business requirements audit package must include testing results in the designated Exchange EDE testing environment. CMS has provided a set of Eligibility Results Toolkits with the eligibility testing scenarios on CMS zONE https://zone.cms.gov/document/business-audit).<br>▪ *Review Standard*: The Auditor must verify and certify the following:<br>– The Auditor was able to successfully complete a series of test eligibility scenarios in the EDE Entity's EDE environment implementation using the Eligibility Results Toolkits. For example, these scenarios may include Medicaid and CHIP eligibility determinations, and different combinations of eligibility determinations for APTC and CSRs. Note: These scenarios do not test, and are not expected to test, every possible question in the Application UI flow for an EDE Entity's selected phase. In addition to reviewing the eligibility results test cases, the Auditor must review the Application UI for compliance as defined above.<br>– The Auditor must test each scenario and verify that the eligibility results and the eligibility process were identical to the expected results and process. The Auditor must provide CMS confirmation that each relevant eligibility testing scenario was successful, that the expected results were received, and must submit the required proof, as defined in the Eligibility Results Toolkits. This will include screenshots, EDNs, and the raw JSON from the Get App API response for the application version used to complete the scenario. Note: EDNs and raw JSONs are required for all required toolkit scenarios; however, screenshots are only required for the highest phase an entity is submitting (for example, a Prospective phase 3 EDE Entity must submit screenshots for the Phase 3 Eligibility Results Toolkit only, but must submit EDNs and raw JSONs for applicable Phase 1, Phase 2, and Phase 3 toolkit scenarios). |
| **API Functional Integration Requirements** | ▪ *Requirement*: EDE Entity must implement the EDE API suite and corresponding UI functionality in accordance with the API specifications and EDE API Companion Guide provided by CMS. The EDE API specifications and EDE API Companion Guide are available on CMS zONE (https://zone.cms.gov/document/api-information).<br>▪ *Review Standard:* The Auditor must complete the set of test scenarios as outlined in the API Functional Integration Toolkit to confirm that the EDE Entity's API and corresponding UI integration performs the appropriate functions when completing the various EDE tasks. For example, the Auditor may have to complete a scenario to verify that a Consumer or Agent and Broker is able to view any SVIs or DMIs that may exist for a Consumer, and confirm that the Consumer or Agent and Broker has the ability to upload documents to resolve any SVIs or DMIs. Some of the test cases require that the Auditor and EDE Entity request CMS to process adjudication actions; the Auditor cannot mark these particular test cases as compliant until evaluating whether the expected outcome occurred after CMS takes the requested action. The Auditor will also need to be aware of the following requirements related to the test scenarios:<br>– Test scenarios in the API Functionality Integration Toolkit must be completed for both the Consumer pathway and the Agent and Broker pathway if an EDE Entity is pursuing approval to use both pathways.<br>– The API Functional Integration Toolkit includes a "Required Evidence" column, Column H, on the "Test Cases" tab. Auditors will need to submit the applicable "Required Evidence," including the complete header and body for each required API request and response, as part of the audit submission. |
| **Application UI Validation** | ▪ *Requirement:* EDE Entity must implement CMS-defined validation requirements within the application. The validation requirements prevent EDE Entity from submitting incorrect data to the Exchange.<br>▪ *Review Standard:* The Auditor must confirm that EDE Entity has implemented the appropriate application field-level validation requirements consistent with CMS requirements. These field-level validation requirements are documented in the FFE Application UI Principles document. |

| Review Category | Requirement and Audit Standard |
|---|---|
| **Section 508-compliant UI** | ▪ *Requirement:* Pursuant to 45 C.F.R. § 155.220(c)(3)(ii)(D) (citing 45 C.F.R. §§ 155.230 and 155.260(b)) and 45 C.F.R. § 156.265(b)(3)(iii) (citing 45 C.F.R. §§ 155.230 and 155.260(b)), Web-brokers and QHP Issuers participating in DE, including all EDE Entities, must implement an eligibility application UI that is Section 508 compliant. A Section 508-compliant application must meet the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)).<br>▪ *Review Standard*: The Auditor must confirm that EDE Entity's application UI meets the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794(d)). The Auditor must verify and certify the following:<br>– Within the Business Requirements Audit Report Template, the Auditor must confirm that the EDE Entity's application UI is Section 508 compliant. No specific report or supplemental documentation is required.<br>– The Auditor may review results produced by a 508 compliance testing tool. If an EDE Entity uses a 508 compliance testing tool to verify that its application UI is 508 compliant, its Auditor must, at a minimum, review the results produced by the testing tool and document any non-compliance, as well as any mitigation or remediation to address the non-compliance. It is not sufficient for an Auditor to state that an EDE Entity complies with this requirement by confirming that the EDE Entity utilized a 508 compliance testing tool. |
| **Non-English-language Version of the Application UI and Communi-cation Materials** | ▪ *Requirement*: In accordance with 45 C.F.R. § 155.205(c)(2)(iv)(B) and (C), QHP Issuers and Web-brokers, including those that are EDE Entities, must translate applicable website content (e.g., the application UI) on Consumer-facing websites into any non-English language that is spoken by a limited English proficient (LEP) population that reaches ten (10) percent or more of the population of the relevant State, as determined in current guidance published by the Secretary of HHS.[39] EDE Entities must also translate communications informing Consumers of the availability of Exchange-generated EDNs; critical communications that the Consumer will no longer receive from the Exchange (i.e., if the EDE Entity has implemented and been approved by CMS to assume responsibility for those communications); and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer's use of its EDE environment into any non-English language that is spoken by an LEP population that reaches ten (10) percent or more of the population of the relevant State, as determined in guidance published by the Secretary of HHS.[40]<br>▪ *Review Standard*: The Auditor must verify and certify the following:<br>– The Auditor must confirm that the non-English-language version of the application UI and associated critical communications are compliant with the Exchange requirements, including the Application UI Toolkit and Communications Toolkit.<br>– The Auditor must verify that the application UI has the same meaning as its English-language version.<br>– The Auditor must also verify that EDE Entity has met all EDE communications translation requirements released by CMS in the Communications Toolkit.<br>– The Auditor must document compliance with this requirement within the Business Requirements Audit Report Template, the Application UI Toolkit, and the Communications Toolkit. In the toolkits, the Auditor can add additional columns for the Auditor compliance findings fields (yellow-shaded columns) or complete the Spanish audit in a second copy of each of the two toolkits. |

[39] Guidance and Population Data for Exchanges, Qualified Health Plan Issuers, and Web-Brokers to Ensure Meaningful Access by Limited-English Proficient Speakers Under 45 CFR §155.205(c) and §156.250 (March 30, 2016) https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Language-access-guidance.pdf and "Appendix A- Top 15 Non-English Languages by State" https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508_update12-20-16.pdf.

[40] Frequently Asked Questions (FAQs) Regarding Spanish Translation and Audit Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with Federally-facilitated Exchanges (FFEs) (June 20, 2018) provides further information regarding translation and audit requirements: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-Spanish-Translation-and-Audit-Requirements.PDF.

| Review Category | Requirement and Audit Standard |
|---|---|
| **EDE Change Management Process** | ▪ *Requirement*: EDE Entity must develop and consistently implement processes for managing changes to the EDE environment relevant to the business requirements audit requirements. This requirement does not replace the evaluation necessary for relevant privacy and security controls. At a minimum, the EDE Entity's change management plan must include the following elements:<br>– A process that incorporates all elements of the Change Notification SOP as referenced in Section XI.A.i, EDE Entity-initiated Change Request Process;<br>– All application and business audit-related changes are thoroughly defined and evaluated prior to implementation, including the potential effect on other aspects of the EDE end-user experience;<br>– A process for defining regression testing scope and developing or identifying applicable testing scenarios;<br>– A process for conducting regression testing;<br>– A process for identifying and correcting errors discovered through regression testing and re-testing the correction;<br>– A process for maintaining separate testing environments and defining the purposes and releases for each environment;<br>– The change management process must be maintained in writing and relevant individuals must be informed on the change management process and on any updates to the process; and<br>– The change management process must include a process, if applicable, for an EDE Entity to update the non-English-language version of the application UI and communication materials for any changes to the application UI or communication materials in the English-language version of the EDE environment.<br>▪ *Review Standard*: The Auditor must evaluate the EDE Entity's change management plan for compliance with the elements and criteria defined above. |
| **Health Reimbursement Arrangement (HRA) Offer Required UI Messaging** | ▪ *Requirement*: Phase 3 EDE Entities, Phase 2 EDE Entities that optionally implement full HRA functionality, and EDE Entities that also offer a classic DE pathway, must implement required UI messaging for qualified individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the qualified individuals consistent with CMS guidance. Required UI messaging for various scenarios are detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document..[41]<br>▪ *Review Standard*: The Auditor must review the EDE Entity's HRA offer implementation to confirm that the required UI messaging content is displayed for each of the relevant scenarios detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document. |

[41] The document FFEs DE API for Web-brokers/Issuers Technical Specifications (Direct Enrollment API Specs) is available on CMS zONE at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

## APPENDIX D: REQUIRED DOCUMENTATION

The below table describes the required artifacts that the EDE Entity must complete for approval during Year 6 of EDE.[42] Additional details about the documentation related to the privacy and security audit (i.e., Interconnection Security Agreement (ISA), Security Privacy Assessment Report, Plan of Actions & Milestones (POA&M), Privacy Impact Assessment, Non-Exchange Entity System Security and Privacy Plan (NEE SSP), Incident Response Plan and Incident/Breach Notification Plan, Contingency Plan, Configuration Management Plan, and Information Security and Privacy Continuous Monitoring Strategy Guide (ISCM Guide)[43] are provided in related CMS guidance. All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

[42] "Year 6 of EDE" refers to the remainder of PY 2023 and PY 2024, including the PY 2024 OEP. The table in Appendix D is an updated combined version of Exhibits 4 and 7 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

[43] These documents are available on CMS zONE at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment.

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| **Notice of Intent to Participate and Auditor Confirmation** | ▪ Once the Prospective Primary and Prospective Phase Change EDE Entity has a confirmed Auditor(s) who will be completing its audit(s), it must notify CMS that it intends to apply to use the EDE pathway for Year 6 of EDE prior to initiating the audit. The email must include the following:<br>– Prospective EDE Entity Name<br>– Auditor Name(s) and Contact Information (Business Requirements and Privacy and Security, if different)<br>– A copy of the executed contract with the Auditor(s) (pricing and proprietary information may be redacted)<br>– EDE Phase (1, 2, or 3)<br>– Prospective EDE Entity Primary Point of Contact (POC) name, email, and phone number. The Primary POC should be a person who is able to make decisions on behalf of the entity<br>– Prospective EDE Entity Technical POC name, email, and phone number. The Technical POC should be a person | ▪ The Prospective Primary and Prospective Phase Change EDE Entity must email directenrollment@cms.hhs.gov<br>▪ Subject line should state: "Enhanced DE: Intent." | Prospective Primary and Prospective Phase Change EDE Entities<br><br>Note: CMS is not collecting notices of intent from prospective Upstream EDE Entities. | March 1 |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| | – who manages technical development<br>– Prospective EDE Entity Emergency POC name, email, and phone number. The Emergency POC should be a person who should be contacted in an emergency situation.[44]<br>– CMS-issued Hub Partner ID | | | |
| **DE Entity Documentation Package—Privacy Questionnaire (or attestation, if applicable, see Submission Requirements column)** | ▪ CMS has provided the privacy questionnaire as part of the DE Entity Documentation Package available on CMS zONE.<br>▪ EDE Entity must populate the privacy questionnaire and return it to CMS for review. | ▪ Submit via the DE/EDE Entity PME Site<br>▪ If an EDE Entity's responses to the privacy questionnaire are unchanged from the EDE Entity's last submission of a privacy questionnaire, the Entity may submit an attestation stating that the previously submitted questionnaire remains accurate.<br>– The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents. | Prospective Primary EDE Entities | Submit with audit submission |

[44] CMS will send EDE related communications to the POCs listed in the EDE Entity's Notice of Intent to Participate. EDE Entities can change these POCs at any time by emailing directenrollment@cms.hhs.gov.

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **DE Entity Documentation Package—Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements column)** | ▪ Submit the URL and text of each privacy policy statement displayed on your website and your website's Terms of Service in a Microsoft Word document or a PDF.<br>▪ The privacy policy and terms of service must be submitted for any EDE Entity's website that is collecting Consumer data as part of the EDE end-user experience. | ▪ Submit via the DE/EDE PME Site<br>▪ If an EDE Entity's privacy policy and Terms of Service remain unchanged from the EDE Entity's last submission of the privacy policy and Terms of Service, the Entity may submit an attestation stating that the previously submitted privacy policy and Terms of Service will remain unchanged.<br>– The attestation must be on company letterhead with a signature from an officer with the authority to bind the entity to the contents | Both Prospective Primary and Prospective Upstream EDE Entities | Prospective Primary EDE Entities: Submit with audit submission.<br><br>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for prospective Upstream EDE Entities, but to be reasonably certain a prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs. |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **EDE Business Agreement** | ▪ EDE Entities must execute the EDE Business Agreement to use the EDE pathway. The agreement must identify the Entity's selected Auditor(s) (if applicable).<br>▪ CMS will countersign the EDE Business Agreement after CMS has reviewed and approved the EDE Entity's business requirements audit and the privacy and security audit. | ▪ Submit via the DE/EDE Entity PME Site | Both Prospective Primary and Prospective Upstream EDE Entities | Prospective Primary EDE Entities: Submit with audit submission.<br><br>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for Prospective Upstream EDE Entities, but to be reasonably certain a Prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs. |
| **DE Entity Documentation Package—Operational and Oversight Information** | ▪ EDE Entities must submit the operational and oversight information to CMS to use the EDE pathway. This form must be filled out completely.<br>▪ The form is an Excel file that the EDE Entity will complete and submit to CMS. | ▪ Submit via the DE/EDE Entity PME Site<br>▪ Prospective Primary EDE Entities will receive an encrypted, pre-populated version of the form from CMS<br>▪ Prospective Upstream EDE Entities will complete a blank version of the form that is available on CMS zONE | Both Prospective Primary and Prospective Upstream EDE Entities | Prospective Primary EDE Entities: Submit with audit submission.<br><br>Prospective Upstream EDE Entities: Submit after the Prospective Primary EDE Entity has submitted its audit. There is no deadline to submit the applicable components of the DE Entity documentation package for Prospective Upstream EDE Entities, but to be reasonably certain a Prospective Upstream EDE Entity will be approved by the start of the OEP, CMS strongly recommends that EDE Entities submit the required documentation no later than October 1 or as soon as feasible to allow time to review prior to activating their Partner IDs. |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **Business Audit Report and Toolkits** | ▪ EDE Entities must submit the Business Requirements Audit Report Template and all applicable toolkits completed by its Auditor(s).<br>▪ See Section VI.B.ii, Business Requirements Audit Resources, Exhibit 5, for more information. | ▪ The EDE Entity and its Auditor(s) must submit the different parts of the Auditor resources package via the DE/EDE Entity PME Site | Prospective Primary EDE Entities, Prospective Phase Change EDE Entities, and their Auditors | April 1 -July 1 (3:00 AM ET) |
| **Training** | ▪ EDE Entities (and their Auditors must complete the trainings as outlined in Section VIII, Required Auditor and EDE Entity Training.<br>▪ The trainings are located on REGTAP (located at the following link: https://www.regtap.info/). | ▪ The person taking the training must complete the course conclusion pages at the end of each module<br>▪ The EDE Entity and Auditor are NOT required to submit anything additional to CMS but must retain a copy of the training confirmation webpage to provide to CMS, if requested | Prospective Primary EDE Entities, Prospective Phase Change EDE Entities, Prospective Upstream EDE Entities, and Auditors | Trainings must be completed by Prospective Primary and Phase Change EDE Entities and Auditors prior to Audit Submission<br><br>Prospective Upstream EDE Entities must complete the training prior to approval to use the EDE pathway |
| **HUB Onboarding Form** | ▪ All EDE Entities must submit a new or updated Hub Onboarding Form to request EDE access. If an EDE Entity does not already have a Partner ID, the Hub will create a Partner ID for the EDE Entity upon receiving the Hub Onboarding Form. | ▪ Follow instructions on the Hub Onboarding Form (located at the following link: https://zone.cms.gov/document/hub-onboarding-form)<br>▪ Send to HubSupport@sparksoftcorp.com | Prospective Primary and Prospective Upstream EDE Entities | Prior to accessing the EDE APIs |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **Application Technical Assistance and Mini Audit Testing Credentials** | ▪ An EDE Entity must provide application technical assistance and mini audit testing credentials to CMS consistent with the process defined in Sections VI.C, Application Technical Assistance and X.D, Audit Submission Compliance Review for Prospective Primary EDE Entities, below. | ▪ Follow instructions on the EDE UI Eligibility Technical Assistance Credentials Form Template on CMS zONE: https://zone.cms.gov/document/eligibility-information | Prospective Primary EDE Entities and Prospective Phase Change EDE Entities | Submit with audit submission date |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **Interconnection Security Agreement (ISA)** | ▪ A Prospective Primary EDE Entity must submit the ISA to use the EDE pathway.<br>▪ CMS will countersign the ISA after CMS has reviewed and approved the EDE Entity's business requirements audit and privacy and security audit. | ▪ A Prospective Primary EDE Entity must submit the ISA via the DE/EDE Entity PME Site.<br>▪ The ISA contains Appendices that must be completed in full for an EDE Entity to be considered for approval.<br>▪ Appendix B of the ISA must detail: (1) all arrangements with Upstream EDE Entities and any related data connections or exchanges, (2) any arrange-ments involving Web-brokers, and (3) any arrangements with downstream agents and brokers that involve limited data collections, as described in Section IV.B, Downstream Third-party Agent and Broker Arrangements.<br>▪ Appendix B of the ISA must be updated and resubmitted as a Primary EDE Entity adds or changes any of the arrangements noted above consistent with the requirements in the ISA. | ▪ Prospective Primary EDE Entities | ▪ Submit with the audit submission |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **Security Privacy Controls Assessment Test Plan (SAP)** | ▪ This report is to be completed by the Auditor and submitted to CMS prior to initiating the audit.<br>▪ The SAP describes the Auditor's scope and methodology of the assessment. The SAP includes an attestation of the Auditor's independence. | ▪ A Prospective EDE Entity and its Auditor must submit the SAP completed by its Auditor via the DE/EDE Entity PME Site. | ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities | ▪ At least thirty (30) Days before commencing the privacy and security audit; during the planning phase |
| **Security Privacy Assessment Report (SAR)** | ▪ This report details the Auditor's assessment findings of the Prospective EDE Entity's security and privacy controls implementation. | ▪ A Prospective EDE Entity and its Auditor must submit the SAR completed by its Auditor via the DE/EDE Entity PME Site. | ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities | ▪ April 1 – July 1 (3:00 AM ET) |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **Plan of Action & Milestones (POA&M)** | ▪ A Prospective EDE Entity must submit a POA&M if its Auditor identifies any privacy and security compliance issues in the SAR.<br>▪ The POA&M details a corrective action plan and the estimated completion date for identified milestones. | ▪ A Prospective EDE Entity and its Auditor must submit the POA&M in conjunction with the SAR via the DE/EDE Entity PME Site.<br>▪ POA&Ms with outstanding findings must be submitted monthly to CMS until all the findings from security controls assessments, security impact analyses, and continuous monitoring activities described in the NEE SSP controls CA-5 and CA-7 are resolved. Prospective EDE Entities can schedule their own time for monthly submissions of the POA&M, but must submit an update monthly to CMS until all significant or major findings are resolved. Thereafter, quarterly POA&M submissions are required as part of the ISCM activities. | ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities | ▪ Initial: April 1 – July 1 (3:00 AM ET)<br>▪ Monthly submissions, as necessary, if outstanding findings.<br>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit quarterly POA&Ms by the last business Day of March, July, September, and December. |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **Risk Acceptance Form** | ▪ The Risk Acceptance Form records the weaknesses that require an official risk acceptance from the organization's Authorizing Official.<br>▪ Before deciding to accept the risks, the relevant NEE's authorities should rigorously explore ways to mitigate the risks. | ▪ Once the risk has been identified and deemed acceptable by the NEE's authorized official, the NEE must complete the entire Risk Acceptance Form and submit the completed form to CMS. The NEE will continue to track all accepted risks in the NEE's official POA&M. | ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities | ▪ The Risk Acceptance Form should be submitted with the POA&M during the regular POA&M submission schedule. |
| **Privacy Impact Assessment (PIA)** | ▪ The PIA will detail the Prospective EDE Entity's evaluation of its controls for protecting PII. | ▪ A Prospective EDE Entity is not required to submit the PIA to CMS. However, per the ISA, CMS may request and review an EDE Entity's PIA at any time, including for audit purposes. | ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities | ▪ Before commencing the privacy and security audit as part of the NEE SSP |
| **Non-Exchange Entity System Security and Privacy Plan (NEE SSP)** | ▪ The NEE SSP will include detailed information about the Prospective EDE Entity's implementation of required security and privacy controls. | ▪ A Prospective Primary EDE Entity must submit the completed NEE SSP via the DE/EDE Entity PME Site before commencing the privacy and security audit.<br>▪ The implementation of security and privacy controls must be completely documented in the NEE SSP before the audit is initiated. | ▪ Prospective Primary and Hybrid Non-Issuer Upstream EDE Entities | ▪ Before commencing the privacy and security audit |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **Incident Response Plan and Incident/ Breach Notification Plan** | ▪ A Prospective EDE Entity is required to implement Breach and Incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures.<br>▪ A Prospective EDE Entity must incorporate these procedures into its own written policies and procedures..[45] | ▪ A Prospective EDE Entity is not required to submit the Incident Response Plan and Incident/Breach Notification Plan to CMS. A Prospective EDE Entity must have procedures in place to meet CMS security and privacy Incident reporting requirements. CMS may request and review an EDE Entity's Incident Response Plan and Incident/Breach Notification Plan at any time, including for audit purposes. | ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities | ▪ Before commencing the privacy and security audit as part of the NEE SSP |

[45] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf.

| | | | | |
|---|---|---|---|---|
| **Annual Penetration Testing** | ▪ The penetration test must include the EDE environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10.<br>▪ Before conducting the penetration testing, the EDE Entity must execute a Rules of Engagement with their Auditor's penetration testing team.<br>▪ The EDE Entity must also notify their CMS designated technical counterparts on their annual penetration testing schedule and must provide the following information to CMS, a minimum of five (5) business Days using the CMS-provided form[46], prior to initiation of the penetration testing:<br>– Period of testing performance (specific times for all penetration testing should be contained in individual test plans);<br>– Target environment resources to be tested (IP addresses, Hostname, URL); and<br>– Any restricted hosts, systems, or subnets that are not to be tested.<br>▪ During the penetration testing, the Auditor's testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment.<br>▪ The penetration testing shall be conducted in the lower environment that mirrors the production environment. | ▪ A Prospective EDE Entity and its Auditor must submit the Penetration Test results with the SAR via the DE/EDE Entity PME Site. | ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities | ▪ Initial: April 1 – July 1 (3:00 AM ET)<br>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities perform penetration testing and submit results to CMS annually, prior to last business Day in July. |

| Document | Description | Submission Requirements | Entity Responsible | Deadline |
|---|---|---|---|---|
| **Vulnerability Scan** | ▪ A Prospective EDE Entity is required to conduct monthly Vulnerability Scans. | ▪ A Prospective EDE Entity and its Auditor must submit the last three months of their Vulnerability Scan Reports, in conjunction with POA&M and SAR via the DE/EDE Entity PME Site.<br>▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&M.<br>▪ Similar findings can be consolidated. | ▪ Prospective Primary, Hybrid Issuer Upstream, and Hybrid Non-Issuer Upstream EDE Entities. | ▪ Initial: April 1 – July 1 (3:00 AM ET)<br>▪ Thereafter, consistent with the ISCM Strategy Guide, EDE Entities must submit Vulnerability Scans annually. |

[46] The Penetration Testing Notification Form is available at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

## APPENDIX E: AUDITOR IDENTIFICATION

EDE Entity agrees to identify, in Part I below, all Auditors selected to complete the Operational Readiness Review (ORR) and any subcontractors of the Auditor(s), if applicable. In the case of multiple Auditors, please indicate the role of each Auditor in completing the ORR (i.e., whether the Auditor will conduct the business requirements audit and/or the privacy and security audit, including the completion of an annual assessment of security and privacy controls by an Auditor, as described in the Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide). Include additional sheets, if necessary. EDE Entity must identify the ISCM Auditor that conducted the ISCM immediately preceding this Agreement's submission and execution.

If an Upstream EDE Entity will contract with an Auditor to audit additional functionality or systems added to its Primary EDE Entity's EDE Environment, pursuant to Section VIII.g or VIII.h of this Agreement, complete Part I to indicate the Auditor(s) that will conduct the business requirements audit and/or privacy and security audit of the additional functionality or systems.

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

## TO BE FILLED OUT BY EDE ENTITY

Primary EDE Entities, Hybrid Issuer Upstream EDE Entities, and Hybrid Non-Issuer Upstream EDE Entities must complete Part I.

### I. Complete These Rows if EDE Entity Is Subject to an Audit (ORR, ISCM, and/or Supplemental Audit)

| | |
|---|---|
| Printed Name and Title of Authorized Official of Auditor 1 | |
| Auditor 1 Business Name | |
| Auditor 1 Address | |
| Printed Name and Title of Contact of Auditor 1 (if different from Authorized Official) | |
| Auditor 1 Contact Phone Number | |
| Auditor 1 Contact Email Address | |
| Subcontractor Name & Information (if applicable) | |
| Audit Role | |
| Printed Name and Title of Authorized Official of Auditor 2 | |
| Auditor 2 Business Name | |
| Auditor 2 Address | |

| | |
|---|---|
| Printed Name and Title of Contact of Auditor 2 (if different from Authorized Official) | |
| Auditor 2 Contact Phone Number | |
| Auditor 2 Contact Email Address | |
| Subcontractor Name & Information (if applicable) | |
| Audit Role | |
| Printed Name and Title of Authorized Official of Auditor 3 | |
| Auditor 3 Business Name | |
| Auditor 3 Address | |
| Printed Name and Title of Contact of Auditor 3 (if different from Authorized Official) | |
| Auditor 3 Contact Phone Number | |
| Auditor 3 Contact Email Address | |
| Subcontractor Name & Information (if applicable) | |
| Audit Role | |

## APPENDIX F: CONFLICT OF INTEREST DISCLOSURE FORM

### TO BE FILLED OUT BY EDE ENTITY

EDE Entity must disclose to the Department of Health & Human Services (HHS) any financial relationships between the Auditor(s) identified in Appendix E of this agreement, and individuals who own or are employed by the Auditor(s), and individuals who own or are employed by a Direct Enrollment (DE) Entity for which the Auditor(s) is conducting an Operational Readiness Review pursuant to 45 C.F.R. § 155.221(b)(4) and (f). EDE Entity must disclose any affiliation that may give rise to any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence.

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

Please describe below any relationships, transactions, positions (volunteer or otherwise), or circumstances that you believe could contribute to a conflict of interest:

☐ Not applicable; EDE Entity is not contracting with an Auditor.
☐ EDE Entity has no conflict of interest to report for the Auditor(s) identified in Appendix E.
☐ EDE Entity has the following conflict of interest to report for the Auditor(s) identified in Appendix E:

1. _____
2. _____
3. _____

## APPENDIX G: APPLICATION END-STATE PHASES

The below table describes each of the three end-state phases for hosting applications using the EDE Pathway.[47] EDE Entity must indicate the end-state phase it has selected in the "Operational and Oversight Information" form provided by CMS. All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions has the meaning provided in 45 C.F.R. § 155.20.

| End State Phases | Description | Benefits |
|---|---|---|
| **Phase 1: Host Simplified Application + EDE API Suite** | EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following:<br>▪ Application filer (and others on application, if applicable) resides in the application state and all dependents have the same permanent address, if applicable<br>▪ Application filer plans to file a federal income tax return for the coverage year; if married plans to file a joint federal income tax return with spouse<br>▪ Application filer (and spouse, if applicable) is not responsible for a child 18 or younger who lives with the Application filer but is not on his/her federal income tax return<br>▪ No household members are full-time students aged 18-22<br>▪ No household member is pregnant<br>▪ All Applicants are U.S. citizens<br>▪ All Applicants can enter Social Security Numbers (SSNs)<br>▪ No Applicants are applying under a name different than the one on his/her Social Security cards<br>▪ No Applicants were born outside of the U.S. and became naturalized or derived U.S. citizens<br>▪ No Applicants are currently incarcerated (detained or jailed)<br>▪ No household members are American Indian or Alaska Native<br>▪ No Applicants are offered health coverage through a job or COBRA<br>▪ No Applicants are offered an individual coverage health reimbursement arrangement (HRA) or qualified small employer health reimbursement arrangement (QSEHRA)<br>▪ No Applicants were in foster care at age 18 and are currently 25 or younger<br>▪ All dependents are claimed on the Application filer's federal income tax return for the coverage year<br>▪ All dependents are the Application filer's children who are single (not married) and 25 or younger<br>▪ No dependents are stepchildren or grandchildren<br>▪ No dependents live with a parent who is not on the Application filer's federal income tax return | Lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope. |

[47] The table in Appendix G is an updated version of Exhibit 3 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

| End State Phases | Description | Benefits |
|---|---|---|
| **Phase 2: Host Expanded Simplified Application + EDE API Suite** | EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following:<br>▪ All scenarios covered by Phase 1<br>▪ Full-time student<br>▪ Pregnant application members<br>▪ Non-U.S. citizens<br>▪ Naturalized U.S. citizens<br>▪ Application members who do not provide an SSN<br>▪ Application members with a different name than the one on their SSN cards<br>▪ Incarcerated application members<br>▪ Application members who previously were in foster care<br>▪ Stepchildren | Second lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope. |
| **Phase 3: Host Complete Application + EDE API Suite** | EDE Entity hosts an application that supports all application scenarios (equivalent to existing HealthCare.gov):<br>▪ All scenarios covered in Phase 2<br>▪ American Indian and Alaskan Native household members<br>▪ Application members with differing home addresses or residing in a State separate from where they are applying for coverage<br>▪ Application members with no home address<br>▪ Application members not planning to file a tax return<br>▪ Married application members not filing jointly<br>▪ Application members responsible for a child age 18 or younger who lives with them, but is not included on the Application filer's federal income tax return (parent/caretaker relative questions)<br>▪ Application members offered coverage through their job, someone else's job, or COBRA<br>▪ Application members with dependent children who are over age 25 or who are married<br>▪ Application members with dependent children living with a parent not on their federal income tax return<br>▪ Dependents who are not sons/daughters<br>▪ Applicants who are offered an individual coverage HRA or QSEHRA | Highest level of effort to implement and audit. EDE Entity would provide and service the full range of Consumer scenarios. Additionally, the EDE Entity would no longer need to redirect Consumers to alternative pathways for complex eligibility scenarios. Please note that the implementation of Phase 3 is comparatively more complex than the other phases and may require more time to implement, audit, and approve. |

## APPENDIX H: TECHNICAL AND TESTING STANDARDS FOR USING THE EDE PATHWAY

All capitalized terms used herein carry the meanings assigned in Appendix B: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix B: Definitions the meaning provided in 45 C.F.R. § 155.20.

(1) EDE Entity must possess a unique Partner ID assigned by the Centers for Medicare & Medicare Services (CMS). EDE Entity must use its Partner ID when interacting with the CMS Data Services Hub (Hub) and the EDE Application Program Interfaces (APIs) for EDE Entity's own line of business.

If EDE Entity uses a Primary EDE Entity's EDE Environment, EDE Entity must use its own Partner ID when interacting with the Hub and the EDE APIs. If EDE Entity is a Primary EDE Entity and provides an EDE Environment to another EDE Entity, as permitted under Section VIII.f, VIII.g, and VIII.h of this Agreement, the Primary EDE Entity must use the Partner ID assigned to the EDE Entity using its EDE Environment for any Hub or EDE API interactions for the other EDE Entity. If EDE Entity is a Primary EDE Entity, it must provide to CMS the Partner IDs of all entities that will implement and use Primary EDE Entity's EDE Environment.

(2) CMS will provide EDE Entity with information outlining EDE API Specifications and with EDE-related Companion Guides, including the EDE Companion Guide, the Federally-facilitated Exchange (FFE) User Interface (UI) Application Principles for Integration with FFE APIs, and the UI Question Companion Guide, which is embedded within the FFE UI Application Principles for Integration with FFE APIs. The terms of these documents are specifically incorporated herein. EDE Entity's use of the EDE Environment must comply with any standards detailed in the EDE API Specifications guidance and the EDE-related Companion Guides.

(3) EDE Entity must complete testing for each Hub-related transaction it will implement, and it shall not be allowed to exchange data with CMS in production mode until testing is satisfactorily passed, as determined by CMS in its sole discretion. Successful testing generally means the ability to pass approved standards, and to process data transmitted by EDE Entity to the Hub. The capability to submit these test transactions must be maintained by EDE Entity throughout the term of this Agreement.

(4) EDE Entity agrees to submit test transactions to the Hub prior to the submission of any transactions to the FFE production system, and to determine that the transactions and responses comply with all requirements and specifications approved by CMS and/or the CMS contractor.

(5) EDE Entity agrees that prior to the submission of any additional transaction types to the FFE production system, or as a result of making changes to an existing transaction type or system, it will submit test transactions to the Hub in accordance with paragraph (3) and (4) above.

(6) EDE Entity acknowledges that CMS requires successful completion of an Operational Readiness Review (ORR) to the satisfaction of CMS, which must occur before EDE Entity is able to execute an ISA with CMS or submit any transactions using its EDE Environment to the FFE production system. The ORR will assess EDE Entity's compliance with CMS' regulatory requirements, this Agreement, and the Interconnection Security Agreement (ISA), including the required privacy and security controls. This Agreement may be terminated or access to CMS systems may be denied for a failure to comply with CMS requirements in connection to an ORR.

(7) Upon approval for a significant change in the EDE Environment, including, but not limited to, initial approval to go-live with an EDE Environment, approval to go-live with an end-state phase change, or approval to proceed with a significant change to EDE Environment functionality, EDE Entity will limit enrollment volume in its production environment in accordance with the scale and schedule set by CMS, in its sole discretion, until CMS has verified the successful implementation of the EDE Entity's EDE Environment in production.

(8) CMS, in its sole discretion, may restrict, delay, or deny an EDE Entity's ability to implement a significant change in the EDE Environment, consistent with paragraph (7) of this Appendix, if an EDE Entity has not maintained compliance with program requirements or the EDE Entity has triggered the conditions for Inactive, Approved Primary EDE Entities (Section IX.v of this Agreement). Failure to maintain compliance with program requirements includes, but is not limited to, an inability to meet CMS-issued deadlines for CMS-initiated Change Requests (Section IX.d of this Agreement) or failure to maintain an EDE Environment that complies with the standards detailed in the EDE API Specifications guidance and the EDE-related Companion Guides.

(9) All compliance testing (Operational, Management and Technical) of EDE Entity will occur at a FIPS 199 MODERATE level due to the Personally Identifiable Information (PII) data that will be contained within EDE Entity's systems.