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)(3)(i), 156.265, and/or 156.1230 to assist Consumers, Applicants, Qualified Individuals, and Enrollees 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:

1. Section 1312(e) of the Patient Protection and Affordable Care Act ("PPACA") 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.

2. Section 1301(a) of the PPACA 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 PPACA and other requirements that an applicable Exchange may establish.

3. 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.

4. 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 PPACA and its implementing regulations permit EDE Entity to perform; and (b) allow EDE Entity to provide such PII and other Consumer information to the FFEs through specific APIs to be provided by CMS.

5. 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 to perform the Authorized Functions described in Section III.a. of this Agreement.

6. 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 principles 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.

7. CMS has adopted privacy and security standards with which the EDE Entity must comply, which are set forth in Appendix A ("Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities"), the CMS Interconnection Security Agreement (ISA) Between Centers for Medicare & Medicaid Services (CMS) and Enhanced Direct Enrollment Entity ("ISA"), and the *Enhanced Direct Enrollment System Security and Privacy Plan*.

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.

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

If EDE Entity is using an Enhanced Direct Enrollment (EDE) Environment it has created for its own use or is providing an EDE Environment for use by other EDE Entities (i.e., "Providers"), EDE Entity must enter into an ISA with CMS. EDE Entity must comply with all terms of the ISA, 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 EDE Entity is using a Provider's EDE Environment, the Provider must supply a System Security Plan (SSP) to each EDE Entity using the Provider's EDE Environment that identifies all "Common Controls" and "Hybrid Controls" implemented in the EDE Environment. All Common and Hybrid security and privacy controls must be documented between each EDE Entity and its Provider as required by the *Enhanced Direct Enrollment System Security and Privacy Plan* section "Common and Hybrid

Controls". Furthermore, Appendix B of the ISA requires Providers to attest that they have documented and shared *Enhanced Direct Enrollment System Security and Privacy Plan* inheritable common and hybrid controls with 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). 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 PPACA. 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:

    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;
    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;
    9. Facilitating an Enrollee's ability to disenroll from a QHP;
    10. Educating Consumers, Applicants, Qualified Individuals or Enrollees 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's ability to report 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 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 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 Web-broker'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. PII Received. 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, 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 Children's Health Insurance Program 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. Ability of Individuals to Limit Collection and Use. EDE Entity agrees to provide the Consumer, Applicant, Qualified Individual, or Enrollee 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 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 applying for a QHP, APTC or CSR eligibility, and for performing Authorized Functions specified in Section III.a. of this Agreement.

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

e. Commitment to Protect Sensitive Information. EDE Entity shall not release, publish, or disclose Consumer personal information and PII to unauthorized personnel, and shall protect such information in accordance with provisions of any laws and regulations governing the adequate safeguarding of sensitive Consumer data, 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 Processing Standards (FIPS) Publication 199.

3. EDE Entity agrees to comply with all federal laws and regulations regarding the handling of sensitive information—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, available at: 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 information 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) for the benefit year beginning January 1, 2021.

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.

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 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 § 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 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 personal information of Consumers, Applicants, Qualified Individuals, and Enrollees. In accordance with section IX.k. 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 or the Web-broker Agreement). However, the termination of EDE Entity's ISA and/or Issuer Agreement or Web-broker Agreement will result in termination of this Agreement. Termination of any of the agreements referenced in this provision will result in 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.

e. Notice to Consumers of Termination of the Interconnection/Agreement, Suspension of Interconnection, and Nonrenewal of Agreement. EDE Entity must provide Consumers 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 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, 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 of the date the termination or suspension of the interconnection will or did occur and direct the Consumer 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, including, but not limited to the Consumer's Application ID, pending actions, and enrollment status, to allow the Consumer to update his or her application and provide the next steps necessary to update the Consumer'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 regarding the Consumer's ability to access his or her application through EDE Entity's website in the future.

   In addition to providing written notice to Consumers, EDE Entity must also prominently display notice of the termination or suspension of the interconnection on EDE Entity's website, including language directing Consumers 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.

VI. Use of EDE Entity's EDE Environment by Downstream and Delegated Entities

EDE Entity may allow third-party Agents or Brokers or other downstream or delegated entities that are 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. However, except as provided in Sections VII.g. and VII.h. of this Agreement, EDE Entity must not provide the capability for the third-party Agents or Brokers or other downstream and delegated entities to use its EDE Environment through the third party's own website or otherwise outside of EDE Entity's approved website. Notwithstanding Sections VII.g. and VII.h., the use of embedding tools and programming techniques, such as iframe technical implementations, that may enable the distortion, manipulation, or modification of the audited and approved EDE Environment and the overall end-user experience developed by a Provider are prohibited unless explicitly approved through the EDE Entity-initiated change request process. The overall EDE end-user experience consists of 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.

VII. Audit Requirements.

a. Operational Readiness Review. 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 Operational Readiness Review (ORR), composed of a business requirements audit and a privacy and security audit. The 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.*[1]

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*, 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 10 percent or more of the state's population, as determined in guidance published by the Secretary of HHS,[2] the Auditor conducting EDE Entity's business requirements audit must also audit the non-English language version of the application UI and any critical communications EDE Entity sends consumers in relation to their use of its EDE Environment for compliance with applicable CMS requirements. EDE Entity must submit the resulting business requirements and privacy and security audit packages to CMS.

[1] This document is available here: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf

[2] *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.

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.[3] 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. 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). If EDE Entity's Auditor(s) subcontracts with another Auditor(s), all Auditor(s) and subcontractors 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.

c. Conflict of Interest. EDE Entity must select an Auditor that is free from 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. 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 a Web-broker or QHP Issuer for which the Auditor is conducting an ORR pursuant to 45 C.F.R. § 155.221(b)(4).[4] EDE Entity must complete the form in Appendix F, if applicable.

d. Auditor Independence and Objectivity. An EDE Entity's Auditor 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. The EDE Entity must not take any actions that impair the independence and objectivity of the EDE Entity's Auditor.

e. Required Documentation. EDE Entity must maintain and/or submit the required documentation detailed in Appendix D, including templates provided by CMS, to

[3] The table in Appendix C is an updated version of Table 2 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."
[4] This subsection was added to 45 C.F.R. § 155.221 as part of the amendments made in the HHS Notice of Benefit and Payment Parameters for 2020 Final Rule (2020 Payment Notice), 84 FR 17454 (April 25, 2019). It will be effective June 24, 2019. Prior to June 24, 2019, the ORR requirements were captured at 45 C.F.R. §155.220(c)(3)(i)(K) for Web-Brokers and 45 C.F.R. § 156.1230(b)(2) for QHP issuers.

CMS in the manner specified in Appendix D.[5] 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 QHP Issuer).

A QHP Issuer EDE Entity may use an EDE Environment provided by another entity (a "Provider"). If a QHP Issuer EDE Entity implements and uses an EDE Environment that is identical to its Provider's EDE Environment, except for minor deviations for branding, the QHP Issuer EDE Entity is not required to submit a business requirements audit package and privacy and security audit package. In all arrangements permitted under this subsection, 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 must be conducted within the confines of the Provider's approved EDE Environment. The QHP Issuer EDE Entity is responsible for ensuring its Provider's EDE Environment complies with all applicable regulations, operational requirements, this Agreement, and the ISA.

In all arrangements permitted under this subsection, the QHP 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, including oversight of the Provider. Any Provider supplying an EDE Environment to a QHP Issuer EDE Entity will be considered a downstream or delegated entity of the EDE Entity. If a QHP Issuer EDE Entity has such a Provider, the EDE Entity must identify that Provider in Appendix E of this Agreement. A QHP Issuer EDE Entity must have a contractual and legally binding relationship with its Provider reflected in a signed, written agreement between the EDE Entity and the Provider.

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 another entity (a "Provider") and, in 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 Provider's EDE Environment, or in addition to the Provider's approved EDE Environment, and to analyze the effect, if any, of those functionalities and systems on the operations and compliance of the Provider's approved EDE Environment. In this scenario, the QHP Issuer 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 QHP Issuer EDE Entity.

[5] The table in Appendix D is a combined version of Exhibits 4 and 6 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

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 QHP Issuer EDE Entity must demonstrate the QHP Issuer EDE Entity's compliance with applicable regulations, operational requirements, this Agreement, and the ISA. The QHP Issuer EDE Entity does not need to submit the Provider's ORR.

CMS considers any changes to the Provider's approved EDE Environment or the overall end-user experience beyond minor branding changes to be the addition of functionality or systems to an approved EDE Environment subject to the requirements of this section. The overall EDE end-user experience consists of 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. In all arrangements permitted under this paragraph, the QHP 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, including oversight of the Provider. Any Provider supplying an EDE Environment to the QHP Issuer EDE Entity will be considered a downstream or delegated entity of the QHP Issuer EDE Entity. If the QHP Issuer EDE Entity has such a Provider, the QHP Issuer EDE Entity must identify that Provider in Appendix E of this Agreement. The QHP Issuer EDE Entity must have a contractual and legally binding relationship with its Provider reflected in a signed, written agreement between the QHP Issuer EDE Entity and the Provider.

A QHP Issuer 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 Non-Issuer EDE Entity will implement its own EDE Environment composed, in part, of an approved EDE Environment provided by another entity (a "Provider") and, in part, of additional functionality or systems implemented by or on behalf of the Non-Issuer EDE Entity, the Non-Issuer EDE Entity must retain an Auditor to conduct part(s) of the ORR relevant to functionalities and systems implemented by the Non-Issuer EDE Entity outside of the Provider's EDE Environment, or in addition to the Provider's approved EDE Environment, and to analyze the effect, if any, of those functionalities and systems on the operations and compliance of the Provider's approved EDE Environment. In this scenario, the 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 Non-Issuer EDE Entity may also be required to submit to CMS an additional supplemental ORR audit package that contains the results of any additional 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 Non-Issuer EDE Entity. The ORR, and additional supplemental ORR audit package that contains the results of the additional supplemental business requirements audit and/or privacy and security audit covering additional functionality or systems implemented by or on behalf of the Non-Issuer

EDE Entity (when required), must demonstrate the Non-Issuer EDE Entity's compliance with applicable regulations, operational requirements, this Agreement, and the ISA. The EDE Entity does not need to submit the Provider's ORR.

CMS considers any changes to the Provider's approved EDE Environment or the overall end-user experience beyond minor branding changes to be the addition of functionality or systems to an approved EDE Environment subject to the requirements of this section. The overall EDE end-user experience consists of 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. In all arrangements permitted under this paragraph, the 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, including oversight of the Provider. Any Provider supplying an EDE Environment to the Non-Issuer EDE Entity will be considered a downstream or delegated entity of the Non-Issuer EDE Entity. If the Non-Issuer EDE Entity has such a Provider, the Non-Issuer EDE Entity must identify that Provider in Appendix E of this Agreement. The Non-Issuer EDE Entity must have a contractual and legally binding relationship with its Provider reflected in a signed, written agreement between the Non-Issuer EDE Entity and the Provider.

A 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.

Depending on the additional functionality and systems added, the Non-Issuer EDE Entity may also need to onboard with CMS as a Web-broker.

VIII. 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).[6] 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 Appendix H.

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*, *Enhanced Direct Enrollment Companion Guide*, and *FFE UI Application Principles for Integration with FFE APIs*. 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

[6] The table in Appendix G is an updated version of Table 1 in the "Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements."

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 Support for Term of Agreement. EDE Entity's EDE Environment must support Consumer-reported Changes in Circumstances (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. If EDE Entity's EDE Environment does not support a Consumer-reported CiC because of the EDE Entity's chosen end-state phase or EDE Entity is no longer operating an EDE Environment, EDE Entity must direct the Consumer to the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]). This provision survives the termination of the Agreement.

c. EDE Entity-initiated Modifications to EDE Environment (EDE Entity-initiated Change Requests). EDE Entity must notify CMS immediately if it intends to make any change to its EDE Environment that affects the information presented to Consumers, Applicants, Qualified Individuals, and Enrollees regarding eligibility, the eligibility application, the eligibility determination, or enrollment processes and to any existing interconnections, including any new updates in processes related to sharing, utilizing, and downloading data.

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). EDE Entity must provide documentation to CMS demonstrating its implementation of applicable CMS-initiated CRs by the CMS-defined 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 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 compliance of EDE Entity's production environment as documented in any CMS-approved or CMS-conducted audits. EDE Entity must provide CMS with credentials to access the testing environment. The testing environment must be appropriately firewalled from the production environment and PII if it does not maintain the privacy and security controls detailed in the ISA and the *Enhanced Direct Enrollment System Security and Privacy Plan*. EDE Entity shall not submit actual PII to the FFE Testing Environments.

   EDE Entity must provide CMS, via the DE Help Desk, with a set of credentials that CMS can use to access the testing environment to complete an audit of 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. Identity Proofing. EDE Entity must meet the identity proofing implementation requirements set forth in Appendix C.

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

h. Post-Eligibility Application Communications. EDE Entity must provide account management functions for Consumers and timely communicate with Consumers 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 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.

i. Accurate Information About Exchanges and Consumer Communications. EDE Entity must meet the requirements related to providing to Consumers accurate information about Exchanges and the Consumer 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.

j. Documentation of Interactions with Consumer Applications or the Exchange. EDE Entity must meet the requirements related to documentation of interactions with Consumer applications or the Exchange set forth in Appendix C.

k. 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.

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

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

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

o. 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 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.

p. Correction of Consumer Application Information. If EDE Entity identifies issues that may affect a consumer's or applicant's eligibility determination or enrollment status, EDE Entity must notify CMS immediately by email to directenrollment@cms.hhs.gov.

CMS may require that EDE Entity submit updated application information to the FFE within 30 days to correct inaccuracies in previously submitted applications and EDE Entity must notify the consumer or applicant of any changes in eligibility or enrollment status as a result of the change.

q. 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, or the request will fail FFE UserID validation. As a reminder, for consumers, the User-ID should be the account UserID for the consumer or a distinct identifier for the consumer.

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" available on CMS zONE at https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

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.

IX. 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 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. EDE Entity shall assume ultimate responsibility for all services and functions described under this Agreement, including those that are assigned or subcontracted to other entities, and must ensure that subcontractors and assignees will perform all functions in accordance with all applicable requirements. EDE Entity shall further be subject to such oversight and enforcement actions for functions assigned to, or activities performed by, subcontractors or assignees 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 assignment of this Agreement or subcontracting of any responsibility hereunder, 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 assignment or subcontracting.

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 through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix I.

d. Incident Reporting Procedures: The EDE entity must implement Incident and Breach Handling procedures as required by the SSP and that are consistent with CMS's Incident and Breach Notification Procedures. Such policies and procedures must identify the 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; 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; and require reporting of any security and privacy Incident or 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 one (1) hour after discovery of the Incident or Breach.

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 PPACA 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. The 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 and for at least ten (10) years after the date this Agreement terminates or expires. 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 the EDE Entity offices, and CMS's review shall not interfere unreasonably with the EDE Entity business activities.

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. 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 delegated or downstream entities must incorporate this Agreement provision.

   This clause survives the expiration or termination of this Agreement.

n. Access to the FFEs. EDE Entity and its assignees or subcontractors—including, employees, developers, agents, representatives, or contractors—cannot remotely connect or transmit data to the FFE or its testing environments, nor remotely connect or transmit data to EDE Entity's systems that maintain connections to the FFE 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.

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, Acting CISO, 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

Statement of Applicability

The security and privacy standards as specified in the *Enhanced Direct Enrollment System Security and Privacy Plan* document and the implementation specifications that are set forth in this Appendix A are consistent with the principles in 45 C.F.R. § 155.260(a)(1) through (a)(6). These standards and implementation specifications are established in accordance with Section 1411(g) of the Patient Protection and Affordable Care Act ("PPACA") (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. All capitalized terms used herein carry the meanings assigned in Appendix B, "Definitions." Any capitalized term that is not defined in Appendix B has the meaning provided in 45 C.F.R. § 155.20.

The 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 and State-based Exchanges on the federal platform ("SBE-FPs"), or directly from Consumers, Applicants, Qualified Individuals, or Enrollees, or these individuals' legal representatives or Authorized Representatives. That agreement and its appendices, including this Appendix A, govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by Non-Exchange Entities in the context of the FFEs and SBE-FPs. In signing that contractual agreement, in which this Appendix A has been incorporated, Non-Exchange Entities agree to comply with the security and privacy standards as specified in the *Enhanced Direct Enrollment System Security and Privacy Plan*[7] and implementation specifications laid out in this document while performing the Authorized Functions outlined in their respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement).

NON-EXCHANGE ENTITY PRIVACY AND SECURITY IMPLEMENTATION SPECIFICATIONS

Non-Exchange Entities must meet the following 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:

(1) Individual Access to PII. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity that maintains and/or stores PII must provide Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives and Authorized Representatives—with a simple and timely means of appropriately accessing PII pertaining to them and/or the person they represent in a physical or electronic readable form and format.

[7] The references in this section to security and privacy controls and implementation standards can be found in the *Enhanced Direct Enrollment System Security and Privacy Plan* located on CMS zONE at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

a. Standard: Individual Access to PII. A Non-Exchange Entity that maintains and/or stores PII must implement policies and procedures that provide access to PII upon request. The EDE Entity must comply with any additional standards and implementation specifications described in EDE SSP IP-2: Individual Access.

i. Implementation Specifications.

1. Access rights must apply to any PII that is created, collected, disclosed, accessed, maintained, stored, and used by the Non-Exchange Entity to perform any of the Authorized Functions outlined in its respective agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement).

2. The release of electronic documents containing PII through any electronic means of communication (*e.g.*, e-mail, web portal) must meet the verification requirements for the release of "written documents" in Section (5)b below.

3. Persons legally authorized to act on behalf of Consumers, Applicants, Qualified Individuals, and Enrollees regarding their PII, including individuals acting under an appropriate power of attorney that complies with applicable state and federal law, must be granted access in accordance with their legal authority. Such access would generally be expected to be coextensive with the degree of access available to the Subject Individual.

4. At the time the request is made, the Consumer, Applicant, Qualified Individual, Enrollee—or these individuals' legal representatives or Authorized Representatives—should generally be required to specify which PII he or she would like access to. The Non-Exchange Entity may assist the Subject Individual in determining his or her information or data needs, if such assistance is requested.

5. Subject to paragraphs (1)a.i.6 and 7 below, a Non-Exchange Entity generally must provide access to the PII in the form or format requested, if it is readily producible in such form or format.

6. The Non-Exchange Entity may charge a fee only to recoup its costs for labor for copying the PII, supplies for creating a paper copy or a copy on electronic media, postage if the PII is mailed, or any costs for preparing an explanation or summary of the PII if the recipient has requested and/or agreed to receive such summary. If such fees are paid, the Non-Exchange Entity must provide the requested copies in accordance with any other applicable standards and implementation specifications.

7. A Non-Exchange Entity that receives a request for notification of or access to PII must verify the requestor's identity in accordance with Section (5)b below.

8. A Non-Exchange Entity must complete its review of a request for access or notification (and grant or deny said notification and/or access) within thirty (30) Days of receipt of the notification and/or access request.

9. Except as otherwise provided in (1)a.i.10, if the requested PII cannot be produced, the Non-Exchange Entity must provide an explanation for its denial of the notification or access request and, if applicable, information regarding the availability of any appeal procedures, including the appropriate appeal authority's name, title, and contact information.

10. A Non-Exchange Entity may deny access to PII that they maintain or store without providing an opportunity for review, in the following circumstances:

    a. If the PII was obtained or created solely for use in legal proceedings or

    b. If the PII is contained in records that are subject to a law that either permits withholding the PII or bars the release of such PII.

(2) 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 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 EDE 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.

(3) 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 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 EDE 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.

(4) Creation, Collection, Disclosure, Access, Maintenance, Storage, and Use Limitations. In keeping with the standards and implementation specifications used by the FFEs, the Non-Exchange Entity must ensure that PII is only created, collected, disclosed, accessed, maintained, stored, and used to the extent necessary to accomplish a specified purpose(s) in the contractual agreement and any appendices. Such information shall never be used to discriminate against a Consumer, Applicant, Qualified Individual, or Enrollee.

a. Standard: Creation, Collection, Disclosure, Access, Maintenance, Storage, and Use Limitations. The EDE Entity must comply with the standards and implementation specifications described in EDE SSP AP-1: Authority to Collect. Other than in accordance with the consent procedures outlined above, the Non-Exchange Entity shall only create, collect, disclose, access, maintain, store, and use PII:

i. In accordance with its published Privacy Notice Statement and any applicable agreements that were in effect at the time the PII was collected, including the consent procedures outlined above in Section (3); and/or

ii. In accordance with the permissible functions outlined in the regulations and agreements between CMS and the Non-Exchange Entity.

b. Standard: Non-discrimination. Non-Exchange Entity should, to the greatest extent practicable, collect PII directly from the Consumer, Applicant, Qualified Individual, or Enrollee, when the information is likely to result in adverse determinations about benefits.

c. Standard: Prohibited Uses and Disclosures of PII.

i. Implementation Specifications.

1. Non-Exchange Entity shall not request information regarding citizenship, status as a national, or immigration status for an individual who is not seeking coverage for himself or herself on any application.

2. Non-Exchange Entity shall not require an individual who is not seeking coverage for himself or herself to provide a Social Security Number (SSN), except if an Applicant's eligibility is reliant on a tax filer's tax return and his or her SSN is relevant to verification of household income and family size.

3. Non-Exchange Entity shall not use PII to discriminate, including, but not limited to, employing marketing practices or benefit designs that will have

the effect of discouraging the enrollment of individuals with significant health needs in QHPs.

(5) Data Quality and Integrity. In keeping with the standards and implementation specifications used by the FFEs, Non-Exchange Entity should take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent such data are necessary for Non-Exchange Entity's intended use of such data, and that such data have not been altered or destroyed in an unauthorized manner, thereby ensuring the confidentiality, integrity, and availability of PII. The EDE Entity must comply with any additional standards and implementation specifications described in EDE SSP DI-1: Data Quality.

a. Standard: Right to Amend, Correct, Substitute, or Delete PII. In keeping with the standards and implementation specifications used by the FFEs, Non-Exchange Entity must offer Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—an opportunity and process to request amendment, correction, substitution, or deletion of PII maintained and/or stored by the Non-Exchange Entity if such individual believes that the PII is not accurate, timely, complete, relevant, or necessary to accomplish an Exchange-related function, except where the PII questioned originated from other sources, in which case the individual should contact the originating source. The EDE Entity must comply with any additional standards and implementation specifications described in EDE SSP IP-3: Redress and IP-4: Complaint Management.

i. Implementation Specifications.

1. Such individuals shall be provided with instructions as to how they should address their requests to the Non-Exchange Entity's Responsible Official, in writing or by telephone. These individuals may also be offered an opportunity to meet with the Responsible Official or his or her delegate(s) in person.

2. Such individuals shall be instructed to specify the following in each request:

a. The PII they wish to correct, amend, substitute or delete; and

b. The reasons for requesting such correction, amendment, substitution, or deletion, along with any supporting justification or evidence.

3. Such requests must be granted or denied within no more than ten (10) working days of receipt.

4. If the Responsible Official (or his or her delegate) reviews these materials and ultimately agrees that the identified PII is not accurate, timely, complete, relevant, or necessary to accomplish the function for which the PII was obtained/provided, the PII should be corrected, amended, substituted, or deleted in accordance with applicable law.

5. If the Responsible Official (or his or her delegate) reviews these materials and ultimately does not agree that the PII should be corrected, amended, substituted, or deleted, the requestor shall be informed in writing of the denial, and, if applicable, the availability of any appeal procedures. If available, the notification must identify the appropriate appeal authority including that authority's name, title, and contact information.

b. Standard: Verification of Identity for Requests to Amend, Correct, Substitute, or Delete PII. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity that maintains and/or stores PII must develop and implement policies and procedures to verify the identity of any person who requests access to, notification of, or modification—including amendment, correction, substitution, or deletion—of PII that is maintained by or for Non-Exchange Entity. This includes confirmation of an individual's legal or personal authority to access, receive notification of, or seek modification—including amendment, correction, substitution, or deletion—of a Consumer's, Applicant's, Qualified Individual's, or Enrollee's PII.

   i. Implementation Specifications.

      1. The requester must submit through mail, via an electronic upload process, or in-person to Non-Exchange Entity's Responsible Official, a copy of one of the following government-issued identification: a driver's license; voter registration card; U.S. military card or draft record; identification card issued by the federal, state, or local government, including a U.S. passport; military dependent's identification card; Native American tribal document; or U.S. Coast Guard Merchant Mariner card.

      2. If such requester cannot provide a copy of one of these documents, he or she can submit two of the following documents that corroborate one another: a birth certificate, Social Security card, marriage certificate, divorce decree, employer identification card, high school or college diploma, and/or property deed or title.

c. Standard: Accounting for Disclosures. Except for those disclosures made to members of Non-Exchange Entity's Workforce who have a need for the record in the performance of their duties, and the disclosures that are necessary to carry out the required functions of Non-Exchange Entity, a Non-Exchange Entity that maintains and/or stores PII shall maintain an accounting of any and all disclosures. The EDE Entity must comply with any additional standards and implementation specifications described in EDE SSP AR-8: Accounting of Disclosures.

   i. Implementation Specifications.

      1. The accounting shall contain the date, nature, and purpose of such disclosures, and the name and address of the person or agency to whom the disclosure is made.

2. The accounting shall be retained for at least ten (10) years after the disclosure, or the life of the record, whichever is longer.

3. Notwithstanding exceptions in Section (1)a.10, this accounting shall be available to Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—on their request per the procedures outlined under the access standards in Section (1) above.

(6) Accountability. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity should adopt and implement the standards and implementation specifications in this document in a manner that ensures appropriate monitoring and other means and methods to identify and report Incidents and/or Breaches. The EDE Entity must comply with any additional standards and implementation specifications described in EDE SSP SE-2 Privacy Incident Response.

a. Standard: Reporting. The Non-Exchange Entity must implement Incident and Breach Handling Procedures that are consistent with CMS' Incident and Breach Notification Procedures[8] and incorporate these procedures in the Non-Exchange Entity's own written policies and procedures.

i. Implementation Specifications. Such policies and procedures would:

1. Identify the Non-Exchange Entity's Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting and managing Incidents or Breaches to CMS;

2. 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; and

3. Require reporting of any security and privacy Incident or 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 one hour after discovery of the Incident or Breach.

b. Standard: Standard Operating Procedures. The Non-Exchange Entity shall incorporate privacy and security standards and implementation specifications, where appropriate, in its standard operating procedures that are associated with functions involving the creation, collection, disclosure, access, maintenance, storage, or use of PII. The EDE Entity must comply with any additional standards

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

and implementation specifications described in EDE SSP AR-1: Governance and Privacy Program.

i. Implementation Specifications.

1. The privacy and security standards and implementation specifications shall be written in plain language and shall be available to all of the Non-Exchange Entity's Workforce members whose responsibilities entail the creation, collection, maintenance, storage, access, or use of PII.

2. The procedures shall ensure the Non-Exchange Entity's cooperation with CMS in resolving any Incident or Breach, including (if requested by CMS) the return or destruction of any PII files it received under the Agreement; the provision of a formal response to an allegation of unauthorized PII use, reuse, or disclosure; and/or the submission of a corrective action plan with steps designed to prevent any future unauthorized uses, reuses, or disclosures.

3. The standard operating procedures must be designed and implemented to ensure the Non-Exchange Entity and its Workforce comply with the standards and implementation specifications contained herein, and must be reasonably designed, taking into account the size and the type of activities that relate to PII undertaken by the Non-Exchange Entity, to ensure such compliance.

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

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

(4) **Auditor** means a person or organization that meets the requirements set forth in this Agreement and contracts with a Web-broker or Issuer for the purposes of conducting an Operational Readiness Review (ORR) in accordance with this Agreement and CMS-issued guidance.

(5) **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.

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

(7) **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.

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

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

(10) **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.

(11) **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.

(12) **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.

(13) **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 Provider.

(14) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a QHP 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.

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

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

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

(18) **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 PII.

(19) **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 PII.

(20) **Direct Enrollment** means the process by which a Web-broker or QHP Issuer may enroll an Applicant in a QHP in a manner that is considered through the Exchange consistent with 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and 156.1230.

(21) **Direct Enrollment (DE) Entity** has the meaning set forth in 45 C.F.R. § 155.20.[9]

[9] This definition was added to 45 C.F.R. § 155.20 as part of the amendments made by the 2020 Payment Notice. It is effective June 24, 2019.

(22) **Enhanced Direct Enrollment (EDE) Entity** means a DE Entity that has been approved by CMS to use the EDE Pathway.

(23) **Enhanced Direct Enrollment (EDE) Environment** means an information technology application or platform provided, owned, and maintained by an EDE Entity or Provider through which an EDE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits consumer information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, and Enrollees in applying for APTC and 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.

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

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

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

(27) **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 PPACA for individual or small group market coverage, including the Federally-facilitated Small Business Health Options Program (**FF-SHOP**). **Federally-facilitated Marketplaces (FFMs)** has the same meaning as FFEs.

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

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

(30) **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.

(31) **Hybrid Control** means those controls that both a Provider and an EDE entity leveraging the Provider's EDE Environment have a shared responsibility of implementing the full control objectives and implementation standards. Hybrid controls refer to a situation where it is possible for an information system to inherit just part of a control from a Provider, with the remainder of the control provided by the EDE entity leveraging the Provider's EDE Environment.

(32) **Hybrid, Non-Issuer Upstream EDE Entity** means a non-issuer EDE Entity that uses the pathway of a Provider and adds functionality or systems to the Provider's EDE Environment such that the Provider's EDE Environment or overall end-user experience is modified beyond minor branding changes.

(33) **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.

(34) **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 Patient Protection and Affordable Care Act.

(4) A program that makes coverage in a Qualified Health Plan through the Exchange with Advance Payments of the Premium Tax Credit 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 PPACA.

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

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

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

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

(39) **Operational Readiness Review (ORR)** means an audit conducted under 45 C.F.R. §§ 155.221(b)(4)[10] and includes the reports submitted by an EDE Entity detailing its compliance with CMS requirements and readiness to implement and use the EDE Environment.

(40) **Patient Protection and Affordable Care Act (PPACA)** means the Patient Protection and 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 Patient Protection and Affordable Care Act.

(41) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and refers to 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.

[10] This subsection was added to 45 C.F.R. § 155.221 as part of the amendments made by the 2020 Payment Notice that will be effective June 24, 2019. Prior to June 24, 2019, the ORR requirements were captured at 45 C.F.R. §155.220(c)(3)(i)(K) for Web-Brokers and 45 C.F.R. § 156.1230(b)(2) for QHP issuers.

(42) **Provider** means an entity that provides access to and allows use of its CMS-approved EDE Environment to other EDE entities. In guidance and program materials, CMS may refer to a Provider as a "primary EDE Entity."

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

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

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

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

(47) **Responsible Official** means an individual or officer responsible for managing a Non-Exchange Entity or Exchange's records or information systems, or another individual designated as an individual to whom requests can be made, or the designee of either such officer or individual who is listed in a Federal System of Records Notice as the system manager, or another individual listed as an individual to whom requests may be made, or the designee of either such officer or individual.

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

(49) **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.

(50) **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.

(51) **State-based Exchange (SBE)** means an Exchange established by a State that receives approval to operate under 45 C.F.R. § 155.105.

(52) **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.

(53) **Streamlined eligibility application user interface (UI)** means the application UI on HealthCare.gov available for Consumers, Applicants, Qualified Individuals, and Enrollees with non-complex eligibility application responses determined by an initial set of eligibility questions for determining the complexity of an applicant's eligibility profile.

(54) **Subject Individual** means that individual to whom a System of Records Notice (SORN) Record pertains.

(55) **System of Records** means a group of Records under the control of any federal agency from which information is retrieved by name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(56) **System of Records Notice (SORN)** means a notice published in the Federal Register notifying the public of a System of Records maintained by a federal agency. The notice describes privacy considerations that have been addressed in implementing the system.

(57) **System of Record Notice (SORN) Record** means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, that individual's education, financial transactions, medical history, and criminal or employment history and that contains that individual's name, or an identifying number, symbol, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger, voice print, or photograph, that is part of a System of Records.

(58) **Web-broker** has the meaning set forth in 45 C.F.R. § 155.20. [11]

(59) **Web-broker Agreement** means the Agreement between a Web-based Entity and CMS for the FFEs and SBE-FPs Individual Market.

(60) **Workforce** means a Non-Exchange Entity's FFE's, or SBE-FP's employees, Agents, 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.

[11] This definition was added to 45 C.F.R. § 155.20 as part of the amendments made by the 2020 Payment Notice that will be effective June 24, 2019. Prior to June 24, 2019, CMS defined web-broker as "an individual agent or broker, group of agents and brokers, or company registered with the FFE that provides a non-Exchange website to assist consumers in the selection and enrollment in QHPs offered through the Exchanges as described in 45 C.F.R. § 155.220(c)(3)."

APPENDIX C: EDE BUSINESS REQUIREMENTS

Review Category	Requirement and Audit Standard
Identity Proofing Implementation	▪ *Requirement*: The EDE Entity must conduct identity proofing for Consumers entering the EDE Pathway for enrollments through both Consumer and in-person Agent/Broker pathways. EDE Entity must conduct identity proofing prior to submitting a Consumer's application to the FFE. If EDE Entity is unable to complete identity proofing of the Consumer, EDE Entity may either direct the Consumer to traditional double-redirect pathway or direct Consumer to the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]. – Remote Identity Proofing/Fraud Solutions Archive Reporting Service (RIDP/FARS) or Third-Party Identity Proofing Services: CMS will make the FFE RIDP/FARS or other third-party identity proofing service available. EDE Entity does not need to use third-party identity proofing if it already uses the approved FFE RIDP service. If EDE Entity uses the FFE RIDP service, it must use the RIDP service only after confirming the Consumer is seeking coverage in a state supported by the FFE/federal platform, but prior to submitting the application. If 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 EDE Entity must be able to produce documentary evidence that each Applicant has been successfully identity 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 EDE Entity if the Applicant creates an account (i.e., username and password) on EDE Entity's website. ▪ Review Standard: – If EDE Entity uses the FFE RIDP service, the Auditor must verify that the EDE Entity has successfully passed testing with the Hub. – If EDE Entity uses a third-party identity proofing service, the Auditor must evaluate and certify the following: o The identity proofing service is FICAM TFS-approved, and o The EDE Entity has implemented the service correctly.
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 EDE Entity is unable to support consistent with the eligibility scenarios supported by 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 the EDE phase EDE Entity implements, EDE Entity must either route the Consumer to the traditional DE double-redirect pathway or direct the Consumer to the FFE (HealthCare.gov or the FFE Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]). ▪ *Review Standard*: The Auditor must verify the following: – The EDE Entity has implemented screening questions—consistent with the requirements in the FFE Application UI Principles document and Application UI Toolkit—to identify Consumers with eligibility scenarios not supported by EDE Entity's EDE Environment. – 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 phase. 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 the CMS zONE EDE Documents and Materials webpage (https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials). Auditors will need to access the FFE Application UI Principles document to conduct the audit. – As explained in the FFE Application UI Principles document, EDE Entity must implement the application in accordance with the FFE requirements. For each applicable eligibility scenario, 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., advanced payments of the premium tax credit [APTC] attestation) must be identical to those of the FFE. – 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) application programming interfaces (APIs) at appropriate intervals within the application process and that 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. 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. ▪ *Review Standard*: The Auditor must review and certify the following: – The FFE Application UI has been implemented in EDE Entity's Environment in accordance with the FFE Application UI Principles document. – The FFE Application UI displays all appropriate eligibility questions and answers from the Application UI Toolkit, including any questions designated as optional. – 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. o 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 scope exceeds the scope of the test cases in the Eligibility Results Toolkits. – 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 use cases and application scenarios, and identifying which scenarios are and are not supported. The disclaimer should direct the Consumer to alternative pathways, such as the traditional DE double-redirect pathway or direct the Consumer to the FFE (HealthCare.gov or the FFE 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 application must display high-level eligibility results, next steps for enrollment, and information about each Applicant's program eligibility, Data Matching Issues (DMIs), special enrollment periods (SEPs), SEP Verification Issues (SVIs), and enrollment steps in a clear, comprehensive and Consumer-friendly way. – EDE Entity must provide Consumers with the CMS-provided Eligibility Determination Notices (EDNs) generated by the FFE any time it submits or updates an application pursuant to requirements provided by CMS in the Communications Toolkit. – 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. The UI requirements related to accessibility of a Consumer's EDN are set forth in the Communications Toolkit. – EDE Entity must provide and communicate status updates and access to information for Consumers to manage their application and coverage. These communications include, but are not limited to, status of DMIs and SVIs, enrollment periods, providing and communicating about new notices generated by the FFE, application and enrollment status, and supporting document upload for DMIs and SVIs. This requirement is detailed in the Communications Toolkit. ▪ *Review Standard*: The Auditor must verify and certify the following: – The EDE Entity's EDE Environment is compliant with the requirements in the Communications Toolkit. – The EDE Entity's EDE Environment notifies Consumers of their eligibility results prior to QHP submission, including when submitting a change in circumstances (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. – 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. – 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.
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 Marketplace-branded communications Consumers may receive with important action items. CMS defines these requirements in the Communications Toolkit. ▪ *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 requirements stated in guidance and the Communications Toolkit.
Documentation of Interactions with Consumer Applications or the Exchange	▪ *Requirement:* EDE Entity must implement tracking metrics 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; handling of action items, such as uploading documents to resolve a DMI). ▪ *Review Standard:* The Auditor must verify EDE Entity's process for determining and tracking when an Agent, Broker, and Consumer has interacted with a Consumer application or taken actions utilizing the EDE Environment. The Auditor must verify and certify the following: – The EDE Entity's Environment tracks, at a minimum, the interactions of Agents, Brokers, and Consumers with a Consumer's account, records, application, or enrollment information. – The EDE Entity's Environment tracks when an Agent, Broker, or Consumer views a Consumer's record, enrollment information, or application information. – The EDE Entity's Environment uses unique identifiers to track and document activities by Consumers, Agents, and Brokers using the EDE Environment. – The EDE Entity's Environment stores this logged information for 10 years.

Review Category	Requirement and Audit Standard
Eligibility Results Testing and SES Testing	▪ *Requirement*: EDE Entity must submit accurate applications through the EDE Pathway that result in accurate and consistent eligibility determinations for the Consumer eligibility scenarios covered by EDE Entity's chosen EDE phase. – The business requirements audit package must include testing results in the designated FFE EDE testing environment. CMS has provided a set of Eligibility Results Toolkits with the eligibility testing scenarios on CMS zONE EDE Documents and Materials webpage (https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials). ▪ *Review Standard*: The Auditor must verify and certify the following: – The Auditor was able to successfully complete a series of test eligibility scenarios using EDE Entity's EDE Environment implementation using the Eligibility Results Toolkits. For example, these scenarios may include Medicaid and Children's Health Insurance Program (CHIP) eligibility determinations, and different combinations of 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. – The Auditor must test each scenario and verify that the eligibility results and the eligibility process were identical to the expected results and process. CMS will require the Auditor to provide confirmation that each relevant eligibility testing scenario was successful, that the expected results were received (as defined in the Eligibility Results Toolkits), and to submit screenshots, EDNs, and FFE Application IDs, when applicable, for each test scenario.
API Functional Integration Requirements	▪ *Requirement*: EDE Entity must implement the EDE API suite in accordance with the API specifications provided by CMS. The EDE API specifications are available on CMS zONE EDE Documents and Materials webpage (https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials). ▪ *Review Standard:* The Auditor must complete a set of Consumer testing scenarios to confirm that EDE Entity's API integration performs the appropriate functions when completing the application; these scenarios are available in the API Functional Integration Toolkit. For example, the Auditor may have to complete a scenario to verify that a Consumer is able to add individuals to the application and, if eligible, to the Consumer's coverage through the CiC process and that the API provides the expected response from the FFE. Some of the test cases require that the Auditor and EDE Entity request CMS to process application actions; the Auditor cannot mark these particular test cases as compliant until evaluating whether the expected outcome occurred after CMS takes the requested action.
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 FFE. ▪ *Review Standard:* The Auditor must confirm that EDE Entity's application has implemented the appropriate 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) and 45 C.F.R. § 156.265(b)(3)(iii) (citing 45 C.F.R. §§ 155.230 and 155.260), 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. § 749(d)). ▪ *Review Standard*: The Auditor must confirm that EDE Entity's application meets the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 749(d)). The Auditor must verify and certify the following: – 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. – 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 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 the 508-Compliant UI requirement by confirming that the EDE Entity utilized a 508 compliance testing tool.
Non-English-language Version of the Application UI and Communication 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 10 percent or more of the population of the relevant state, as determined in current guidance published by the Secretary of HHS.[12] 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 (to be identified by CMS); 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 10 percent or more of the population of the relevant state, as determined in guidance published by the Secretary of HHS.[13] ▪ *Review Standard*: The Auditor must verify and certify the following: – The Auditor must confirm that the non-English-language version of the application UI and associated critical communications are compliant with the FFE requirements, including the Application UI Toolkit and Communications Toolkit. – The Auditor must verify that the application UI has the same meaning as its English-language version. – The Auditor must also verify that EDE Entity has met all EDE communications translation requirements released by CMS in the Communications Toolkit. – 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.

[12] 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.

[13] *Frequently Asked Questions (FAQs) Regarding Spanish Translation and Audit Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with 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
Agent and Broker Identity Proofing Verification	▪ *Requirement:* Agent/Broker Identity Proofing Requirements. EDE Entity must implement Agent and Broker identity verification procedures that consist of the following requirements: – EDE Entity must provide User-Id of the requester in the header for each EDE API call. For Agents and Brokers, the User-Id must exactly match the FFE-assigned User-Id for the Agent or Broker, or the request will fail FFE User-Id validation. For Consumers, 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. o 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. – EDE Entity must identity proof all Agents and Brokers prior to allowing the Agents and Brokers to use its EDE Environment. EDE Entity may conduct identity proofing in one of the following ways: – Use the FFE-provided Remote Identity Proofing/Fraud Solutions Archive Reporting Service (RIDP/FARS) APIs to remotely identity proof Agents and Brokers; OR – Manually identity proof Agents and Brokers following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE EDE Documents and Materials webpage (https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials). – 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. ▪ *Review Standard:* For audits submitted during plan year 2019, for verification of these procedures, the Auditor must verify and certify the following: – EDE Entity's inclusion of the appropriate Agent/Broker and Consumer User-Id fields in the EDE and Fetch Eligibility API calls. – EDE Entity's process for identity proofing an Agent or Broker prior to allowing an Agent or Broker to use its EDE Environment. – 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.

APPENDIX D: REQUIRED DOCUMENTATION

The below table describes the required artifacts that the EDE Entity must complete. 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, System Security Privacy Plan, Incident Response Plan and Incident/Breach Notification Plan, Contingency Plan, Configuration Management Plan, and Information Security and Privacy Continuous Monitoring Strategy Guide (ISCM Guide))[14] are provided in related CMS guidance.

Document	Description	Submission Requirements	Entity Responsible (Upstream/Provider/ Both Provider and Upstream/Auditor)	Deadline
Notice of Intent to Participate and Auditor Confirmation	▪ Once the prospective 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 PY 2019 or PY 2020 *prior to initiating the audit.* The email must include the following: – Prospective EDE Entity Name – Auditor Name(s) and Contact Information (Business Requirements and Privacy and Security, if different) – EDE Phase (1, 2, or 3) – Prospective EDE Entity Primary Point of Contact (POC) name, email, and phone number – Prospective EDE Entity Technical POC name, email, and phone number – Prospective EDE Entity Emergency POC name, email, and phone number – CMS-issued Hub Partner ID	▪ The QHP issuer or web-broker should email directenrollment@cms.hhs.gov ▪ Subject line should state: "Enhanced DE: Intent."	Provider	February 28, 2019

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

Document	Description	Submission Requirements	Entity Responsible (Upstream/Provider/ Both Provider and Upstream/Auditor)	Deadline
Confirmation of Upstream Entities	▪ CMS requires confirmation of any upstream EDE Entities that will use a Provider's EDE Environment from both the Provider and each upstream EDE Entity. ▪ *For upstream EDE Entities*: The email from the upstream EDE Entity must include the following: – Name of EDE Entity providing your EDE Environment – Primary POC name, email, and phone number – Emergency POC name, email, and phone number	▪ The QHP issuer or web-broker should submit the documentation through the secure portal as part of the audit submission package, or subsequently if the upstream relationship is established after the audit submission to the DE Help Desk directenrollment@cms.hhs.gov. ▪ CMS will provide an Upstream Documentation Package on CMS zONE that will include the required documentation upstream EDE Entities must submit to CMS.	Both Provider and Upstream	If known, Providers will notify CMS as part of the audit submission. After audit submission, CMS will review and approve upstream EDE Entities on a rolling basis.
Privacy Questionnaire (or attestation, if applicable, see Submission Requirements)	▪ CMS will provide the questionnaire to each prospective EDE Entity as part of the audit submission package. ▪ If a prospective EDE Entity submitted a questionnaire during a prior application process, the Entity may submit an attestation if the responses to the privacy questionnaire will remain unchanged from the language already submitted to CMS.	▪ Submit via the secure portal ▪ If an EDE Entity submitted a question-naire during a prior application process, the Entity may submit an attestation if the responses to the privacy questionnaire will remain unchanged from the language already submitted to CMS.	Provider	Submitted with audit submission, or no later than June 30, 2019.
Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements)	▪ 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.	▪ Submit via the secure portal ▪ If an EDE Entity was previously approved to use EDE, the Entity may submit an attestation if the privacy policy state-ment(s) and Terms of Service will remain unchanged from the language previously submitted to CMS.	Both Provider and Upstream	Submitted with Audit Submission, or no later than June 30, 2019.

Document	Description	Submission Requirements	Entity Responsible (Upstream/Provider/ Both Provider and Upstream/Auditor)	Deadline
Training	▪ Prospective EDE Entities and Auditors must complete the trainings outlined in Section VIII. 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. ▪ The prospective EDE Entity and Auditor are NOT required to submit anything additional to CMS but must print a copy of the training confirmation webpage to provide to CMS, if requested.	Provider, Auditor CMS recommends that representatives from any upstream EDE Entities take the trainings outlined in Section VIII.	Trainings must be completed by Providers and Auditors prior to Audit Submission
EDE Business Agreement	▪ Providers and upstream EDE Entities must submit the EDE Business Agreement to use the EDE Pathway. The agreement must identify the Entity's selected Auditor. ▪ CMS will countersign the EDE Business Agreement after CMS has reviewed and approved the business requirements audit and the privacy and security audit.	▪ Submit via the secure portal	Both Provider and Upstream	Submitted with Audit Submission, or no later than June 30, 2019.
Business Audit Report and Toolkits	▪ A prospective EDE Entity must submit the Business Requirements Audit Report Template and all applicable toolkits completed by its Auditor. ▪ See below "Business Requirements Audit Resources" for more information.	▪ A prospective EDE Entity and its Auditor must submit the different parts of the Auditor resources package via the secure portal.	Provider	April 1, 2019– June 30, 2019
HUB Onboarding Form (for Providers with upstream EDE Entities only)	▪ An EDE Entity that has upstream EDE Entities must provide a HUB Onboarding Form to CMS detailing the information to acquire Partner IDs for all upstream EDE Entities.	▪ Follow instructions on form (located at the following link: https://zone.cms.gov/document/hub-onboarding-form)	Provider	As upstream EDE Entities are added
Interconnection Security Agreement (ISA)	▪ A prospective EDE Entity must submit the ISA to use the EDE Pathway. ▪ CMS will countersign the ISA after CMS has reviewed and approved the business requirements audit and privacy and security audit.	▪ A prospective EDE Entity must submit the ISA via the secure portal.	Provider	April 1, 2019– June 30, 2019

Document	Description	Submission Requirements	Entity Responsible (Upstream/Provider/ Both Provider and Upstream/Auditor)	Deadline
Security Privacy Controls Assessment Test Plan (SAP)	▪ This report is to be completed by the Auditor and submitted to CMS prior to the audit. ▪ 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.	Provider	Before commencing the privacy and security audit; during a prospective EDE Entity and the Auditor 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 secure portal.	Provider	April 1, 2019– June 30, 2019
Plan of Actions & 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. ▪ 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 secure portal. ▪ POA&Ms with outstanding findings must be submitted monthly to CMS until all significant vulner-abilities are addressed. The POA&M must be submitted quarterly thereafter.	Provider	April 1, 2019– June 30, 2019
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.	Provider	Before commencing the privacy and security audit as part of the EDE SSP
System Security and Privacy Plan (SSP)	▪ The SSP will include detailed information about the prospective EDE Entity's implementation of required security and privacy controls.	▪ A prospective EDE Entity is not required to submit the SSP to CMS. However, per the ISA, CMS may request and review an EDE Entity's SSP at any time, including for audit purposes. ▪ The implementation of security and privacy controls must be completely docu-mented in the SSP before the audit is initiated.	Provider	Before commencing the privacy and security audit

Document	Description	Submission Requirements	Entity Responsible (Upstream/Provider/ Both Provider and Upstream/Auditor)	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. ▪ A prospective EDE Entity must incorporate these procedures into its own written policies and procedures.[15]	▪ A prospective EDE Entity is not required to submit the Incident Response Plan and Incident/Breach Notification Plan to CMS. However, per the ISA, CMS may request and review an EDE Entity's Incident Response Plan and Incident/Breach Notification Plan at any time, including for audit purposes.	Provider	Before commencing the privacy and security audit as part of the EDE SSP
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 secure portal.	Provider	April 1, 2019–June 30, 2019
Information Security and Privacy Continuous Monitoring Strategy Guide (ISCM Guide)	▪ The ISCM Guide describes CMS's strategy for EDE Entities following the initial approval of the Request to Connect (RTC). This guide conveys the minimum requirements for EDE Entities that implement an ISCM program for their systems and to maintain ongoing CMS RTC approval.	▪ Monthly, quarterly, and annual reporting summaries. ▪ Subset of security and privacy core controls that must be tested annually and reported to CMS.	Provider	Ongoing

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

APPENDIX E: AUDITOR IDENTIFICATION

EDE Entity agrees to identify, in Part I below, the Auditor(s) 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). Include additional sheets, if necessary.

If EDE Entity is accounted for under an ORR provided by another entity (a "Provider"), pursuant to Section VII.f. of this Agreement, complete Part II below. If EDE Entity will add additional functionality or systems to its Provider's EDE Environment, pursuant to Section VII.g. or VII.h. of this Agreement, complete Part III to indicate the Auditor(s) that will conduct the business requirements audit and/or privacy and security audit of the additional functionality or systems. Regardless of the specific circumstances of the EDE Entity's implementation, each EDE Entity must attest to the accuracy of this information by signing in Part IV below.

TO BE FILLED OUT BY EDE ENTITY

Is the EDE Entity using the Provider's EDE Environment with only minor deviations for branding (see Section VII.f.)? If yes, complete Part II.

Is the EDE Entity adding additional functionality or systems to the Provider's EDE Environment (see Section VII.g. or VII.h.)? If yes, complete Part III.

All EDE Entities must complete Part IV.

I. Complete These Rows if EDE Entity Is Subject to an Audit

Printed Name and Title of Authorized Official of Auditor 1	
Auditor 1 Name	
Auditor 1 Address	
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 Name	
Auditor 2 Address	
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 (if applicable)	
Auditor 3 Name (if applicable)	
Auditor 3 Address (if applicable)	
Auditor 3 Contact Phone Number (if applicable)	
Auditor 3 Contact Email Address (if applicable)	
Subcontractor Name & Information (if applicable)	
Audit Role (if applicable)	

II. Complete These Rows if EDE Entity's EDE Environment Is Provided by a Provider

Name of Provider Entity Providing EDE Environment	
Address of Provider Entity Providing EDE Environment	
Printed Name and Title of Authorized Official of Provider Entity Providing the EDE Environment	
Contact Information for Authorized Official of Provider Entity Providing the EDE Environment	
Is the Provider Entity Providing an ORR Report for the EDE Environment?	

If the EDE Entity is completing Part II because its EDE Environment is provided by a Provider, EDE Entity must attest to the following by signing below:

EDE Entity's EDE Environment uses an identical EDE Environment to that provided by the Provider EDE Entity, except for minor branding discrepancies, as allowed under Section VII.f. EDE Entity understands that if it plans to make any changes to the EDE Environment, Section VIII.c. requires that the EDE Entity notify CMS of these changes, and, consistent with these above provisions, the EDE Entity may be required to obtain a third-party, independent auditor to conduct an audit to verify the compliance of the EDE Environment with those changes.

III. Complete These Rows if EDE Entity Is Adding Functionality or Systems to a Provider's EDE Environment

Is EDE Entity an Issuer?	
Name of Provider Entity Providing EDE Environment	
Address of Provider Entity Providing EDE Environment	
Printed Name and Title of Authorized Official of Provider Entity Providing the EDE Environment	

Contact Information for Authorized Official of Provider Entity Providing the EDE Environment	
Is the Provider Entity Providing an ORR Report for its EDE Environment?	
Describe the full scope of changes that the EDE Entity is making to its Provider's EDE Environment consistent with Section VII.g. and VII.g.1.	
Printed Name and Title of Authorized Official of Auditor 1	
Auditor 1 Name	
Auditor 1 Address	
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 Name	
Auditor 2 Address	
Auditor 2 Contact Phone Number	
Auditor 2 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	

IV. EDE Entity's Signature Attesting to the Accuracy of this Information

Signature of Authorized Official of EDE Entity

Date

Printed Name and Title of Authorized Official of EDE Entity

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), and individuals who own or are employed by the Auditor(s), and individuals who own or are employed by a Web-broker or Qualified Health Plan (QHP) Issuer for which the Auditor(s) is conducting an Operational Readiness Review pursuant to 45 C.F.R. § 155.221(b)(4).[16] 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.

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 (see Appendix E).
- ○ EDE Entity has no conflict of interest to report.
- ○ EDE Entity has the following conflict of interest to report:

1. _____
2. _____
3. _____

I hereby certify that the information set forth above is true and complete to the best of my knowledge.

_____ _____

Signature of Authorized Official of EDE Entity Date

_____

Printed Name and Title of Authorized Official of EDE Entity

[16] This subsection was added to 45 C.F.R. § 155.221 as part of the amendments made by the 2020 Payment Notice that will be effective June 24, 2019. Prior to June 24, 2019, the ORR requirements were captured at 45 C.F.R. § 155.220(c)(3)(i)(K) for Web-Brokers and 45 C.F.R. § 156.1230(b)(2) for QHP issuers.

APPENDIX G: APPLICATION END-STATE PHASES

The below table describes each of the three end-state phases for hosting applications using the EDE Pathway. EDE Entity must indicate the end state phase it has selected in Appendix H.

End State Phases	Description	Benefits
Phase 1: Host Simplified Application (App 2.0) + EDE API Suite	EDE Entity hosts an application that cannot support all application scenarios, but will support only a subset of application scenarios equivalent to the current streamlined application user interface (App 2.0) implementation.	EDE Entity could leverage the application created for proxy DE (if applicable) to reduce the amount of UI implementation required.
Phase 2: Host Expanded Simplified Application (App 2.0+) + EDE API Suite	EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following: ▪ All scenarios covered by App 2.0 ▪ Full-time student ▪ Pregnant application members ▪ Non-U.S. citizens ▪ Naturalized U.S. citizens ▪ Application members who do not provide a Social Security Number (SSN) ▪ Application members with a different name than the one on their SSN cards ▪ Incarcerated application members ▪ Application members who previously were in foster care ▪ Stepchildren	EDE Entity could leverage the application created for proxy DE (if applicable) to reduce the amount of UI implementation required. 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 Classic application/App 3.0): ▪ All scenarios covered in Phase 2 ▪ American Indian and Alaskan Native application members ▪ Application members with differing home addresses or residing in a state separate from where they are applying for coverage ▪ Application members with no home address ▪ Application members not planning to file a tax return ▪ Married application members not filing jointly ▪ Application members responsible for a child 18 or younger who lives with them but is not included on federal tax return (parent/caretaker relative questions) ▪ Application members offered coverage through their job, someone else's job, or COBRA ▪ Application members with dependent children who are over 25 or who are married ▪ Application members with dependent children (under 21) who are not applying for coverage ▪ Application members with dependent children living with a parent not on their federal tax return ▪ Dependents who are not sons/ daughters	EDE Entity would provide and service the full span of Consumer scenarios. Additionally, the entity would no longer be required to support integration with the standard DE security assertion markup language (SAML) double redirect process.

APPENDIX H: END-STATE PHASE SELECTION

TO BE FILLED OUT BY PRIMARY OR PROVIDER EDE ENTITY

(1) Application End-State Phase Selection. EDE Entity will implement the following end-state phase for its EDE Environment as represented in the Operational Readiness Review submitted with this EDE Business Agreement (select one) for plan year 2019 and 2020 (select one):

- (●) Phase 1
- ( ) Phase 2
- ( ) Phase 3

As explained in Section VIII.a. of this Agreement, EDE Entity may not switch the end-state phase it has selected without first consulting and receiving approval from the Centers for Medicare & Medicare Services (CMS). Any change in supported end-state phase may require additional verification from an independent third-party auditor.

APPENDIX I: TECHNICAL AND TESTING STANDARDS FOR USING THE EDE PATHWAY

(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 another entity's (a Provider'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 Provider and provides an EDE Environment to another EDE Entity, as permitted under Section VII.f. or VII.g. of this Agreement, the Provider 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 Provider, it must provide to CMS the Partner IDs of all entities that will implement and use Provider'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) 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.