

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 8-K

CURRENT REPORT

PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

DATE OF REPORT (DATE OF EARLIEST EVENT REPORTED): October 31, 2017

eHealth, Inc.

(Exact name of registrant as specified in its charter)

Delaware
(State or other jurisdiction of
incorporation)

001-33071
(Commission File Number)

56-2357876
(I.R.S. Employer
Identification No.)

440 East Middlefield Road
Mountain View, California 94043
(Address of principal executive offices) (Zip code)

(650) 584-2700
Registrant's telephone number, including area code
Not Applicable
(Former name or former address if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

- ☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
- ☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
- ☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
- ☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (17 CFR §230.405) or Rule 12b-2 of the Securities Exchange Act of 1934 (17 CFR §240.12b-2).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 7.01 Regulation FD Disclosure.

DE Proxy Direct Enrollment Agreement with the Centers for Medicare & Medicaid Services

On October 31, 2017, eHealth, Inc. (the “Company”) (through its subsidiary eHealthInsurance Services, Inc.) entered into a Proxy Direct Enrollment Agreement (the “DE Proxy Agreement”) with the Centers for Medicare and Medicaid Services (the “CMS”). CMS is the government agency that is responsible for the management and oversight of the Federally-facilitated marketplace (“FFM”) created under the Patient Protection and Affordable Care Act of 2010, as amended (the “Affordable Care Act”).

By signing the DE Proxy Agreement, the Company may utilize a new qualified health plan (“QHP”) enrollment process through the FFM that would allow the Company to enroll customers into QHPs and apply for advanced payment of premium tax credits through the FFM without leaving the Company’s website during the open enrollment period for 2018 coverage. The DE Proxy Agreement defines the set of information that the Company may create, collect, disclose, access, maintain, store and use and places restrictions on the Company’s use and disclosure of such information. The Company must also ensure that the application questions and the order they are asked on the Company’s website duplicate the questions and order on the FFM. Moreover, the DE Proxy Agreement contains privacy and security standards and implementation specifications that the Company must meet in order to have access, and continue to have access, to the enrollment pathway. The Company must also conduct identity proofing for consumers prior to submitting the application to the FFM. The term of the DE Proxy Agreement ends on the day before the first day of the open enrollment period for the benefit year beginning January 1, 2019, after which the agreement may be renewed for subsequent and consecutive one (1) year periods subject to CMS’ sole and absolute discretion. In addition, the DE Proxy Agreement may be terminated for convenience upon thirty (30) days’ prior written notice by either the Company or CMS and may be terminated for cause by CMS in accordance with termination provisions of the DE Proxy Agreement. Moreover, CMS may amend the DE Proxy Agreement upon 30-days’ notice to reflect changes in applicable law or regulations.

While the Company has entered into the DE Proxy Agreement and set up systems designed to use the direct enrollment pathway under the DE Proxy Agreement, there are risks and uncertainties relating to the Company’s ability to enroll individuals into QHPs through the FFM and to assist those individuals in applying for subsidies. Among other things, the Company must satisfy, and continue to satisfy, the requirements contained in the DE Proxy Agreement, other relevant agreements with CMS, and applicable laws, regulations and regulatory guidance; maintain a compliant web platform incorporating those requirements; obtain qualified health plan information from the Company’s health insurance carrier partners and CMS and incorporate it into its web platform; maintain a privacy and security program to conform to the privacy and security requirements required by the CMS; and successfully maintain the direct enrollment pathway with the FFM so that information may be passed to and from the Company and the FFM relating to enrollment in QHP and subsidy eligibility. In addition, the Company is dependent upon the operability of the FFM website and systems to be able to enroll individuals in QHPs through the FFM, and any change to, failure of or interruption in the availability of the FFM systems could harm the ability of the Company to enroll individuals into QHPs. The Company depends upon the FFM for a number of other things relating to the Company’s ability to enroll individuals into QHPs, including integration of the Company’s systems with the FFM’s systems as well as certain qualified health plan information required under the applicable regulations to be displayed on the Company’s website.

The foregoing description of the terms of the DE Proxy Agreement does not purport to be complete. The DE Proxy Agreement is qualified in their entirety by reference to the full text of the DE Proxy Agreement attached hereto as Exhibit 99.1. In addition, the discussion of aspects of the Affordable Care Act and related regulations are merely summaries of aspects of complex laws and do not purport to be complete summaries.

This Current Report on Form 8-K contains forward-looking statements, including statements regarding the Company’s ability to enroll individuals in QHPs and apply for advanced payment of premium tax credits through the FFM without leaving the Company’s website during the open enrollment period for 2018 coverage, the obligation of eligible individuals to purchase QHPs through a government-run health insurance exchange and the Affordable Care Act and the related regulation. These forward-looking statements involve certain risks and uncertainties that could cause actual results to differ materially from those indicated in such forward-looking statements, including, but not limited to, the Company’s ability to enroll individuals in qualified health plans through the FFM without leaving the Company’s website; the Company’s ability to maintain the DE Proxy Agreement and other agreements with the CMS which need to be renewed every year; the Company’s ability to satisfy the conditions and requirements contained in the DE Proxy Agreement and applicable laws, regulations and regulatory guidance; the Company’s ability to maintain a compliant web platform incorporating the requirements of the DE Proxy Agreement, any other relevant agreements with CMS, and applicable laws, regulations and

regulatory guidance; the Company’s ability to obtain qualified health plan information from the Company’s health insurance carrier partners and CMS and incorporate it into its web platform; the Company’s ability to maintain a privacy and security program to conform to the privacy and security requirements of the DE Proxy as well as laws, regulations and regulatory guidance applicable to the Company acting as a WBE; the availability and reliability of the FFM website and systems; and the Company’s ability to timely meet the applicable requirements and potential changes in laws, regulations and regulatory guidance. Other risks and uncertainties that can affect actual results are included under the captions “Risk Factors” and “Management’s Discussion and Analysis of Financial Condition and Results of Operations” in our Annual Report on Form 10-K for the year ended December 31, 2016 and our most recent Quarterly Report on Form 10-Q, which are on file with the SEC and are available on the investor relations page of the Company’s website at <http://www.ehealthinsurance.com> and on the Securities and Exchange Commission’s website at www.sec.gov . All information provided in this Current Report on Form 8-K is as of the date of its filing, and we undertake no duty to update this information unless required by law. The information in Item 7.01 of this Current Report on Form 8-K and the exhibits attached hereto shall be deemed “furnished” and shall not be deemed “filed” for purposes of Section 18 of the Securities Exchange Act of 1934, as amended. Except as shall be expressly set forth by specific reference in such filing, the information contained herein and in the accompanying exhibits shall not be incorporated by reference into any filing with the Securities and Exchange Commission made by the Company, whether made before or after the date hereof, regardless of any general incorporation language in such filing.

Item 9.01. Financial Statements and Exhibits

(d) Exhibits.

Exhibit Number	Description
99.1	Proxy Direct Enrollment Agreement Between 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.
	.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, as amended, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

Date: October 31, 2017

eHealth, Inc.

By: /s/ Scott Giesler

Scott Giesler

Senior Vice President, General Counsel & Secretary

EXHIBIT INDEX

Exhibit Number	Description
99.1	Proxy Direct Enrollment Agreement Between 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. .

**PROXY DIRECT ENROLLMENT AGREEMENT BETWEEN 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 PROXY 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 ("FFE") and the operation of the Federal eligibility and enrollment platform relied upon by certain State-based Exchanges for their eligibility and enrollment functions ("SBE-FPs"), including the CMS Data Services Hub ("Hub"), and eHealthInsurance Services, Inc. (hereinafter referred to as "Direct Enrollment (DE) Entity"), that 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 Credits ("APTCs") and Cost-sharing Reductions ("CSRs"); applying for enrollment in Qualified Health Plans ("QHPs") offered on the FFEs or SBE-FPs; completing enrollment in QHPs offered on the FFEs or SBE-FPs; and providing related Customer Service. CMS and DE Entity 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 and 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 APTCs 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 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 an application programming interface to DE Entity that will enable DE Entity to establish a secure connection with the Hub. The application programming interface will enable the secure transmission of key eligibility and enrollment information between CMS and DE Entity.
4. To facilitate the operation of the FFEs and SBE-FPs, CMS desires to: (a) allow DE 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 the DE 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 DE Entity to perform; (b) allow DE Entity to provide such PII and other consumer information to the FFEs through a specific Proxy DE Pathway to be provided by CMS; and (c) permit DE Entity to implement an automation tool for the purposes of completing the FFE streamlined application user interface (UI) for eligibility.

5. DE Entity is approved to use the specific Proxy DE Pathway provided by CMS consistent with applicable regulations and this Agreement. DE Entity desires to use the specified Proxy DE Pathway provided by CMS 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 II.a of this Agreement. This Agreement is limited to the use of the specific Proxy DE Pathway provided by CMS, reflects the consent and intent of the parties to establish an electronic connection between the information technology networks and systems of the parties, and establishes a commitment to protect data that is exchanged between the networks or processed and stored on the systems that reside on the networks. Through this Agreement, both parties shall minimize the susceptibility and exposure of their connected systems and networks to system privacy and security risks and aid in mitigation and recovery from security and privacy incidents.
6. DE Entity has contracted with an Auditor consistent with this Agreement's provisions and applicable regulatory requirements to verify and attest to DE Entity's compliance with the terms of this Agreement, the DE Entity's respective agreements with CMS (QHP Issuer Agreement and the Web-broker Agreement), and applicable program requirements.
7. 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. § 156.260(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).
8. CMS, in the administration of the FFEs, the federal platform for SBE-FPs, and the Hub, has adopted privacy and security standards, as set forth in Appendix B, "Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities," and Appendix E, "Security and Privacy Controls."

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 C, "Definitions." Any capitalized term that is not defined herein or in Appendix C has the meaning provided in 45 C.F.R. § 155.20.

II. Acceptance of Standard Rules of Conduct.

DE Entity and CMS are entering into this Agreement to satisfy the requirements under 45 C.F.R. § 155.260(b)(2). DE 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 DE Entity for purposes of the PPACA. DE 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 these standards are less stringent than privacy and security standards applied to DE Entity through any existing agreements with CMS, the more stringent privacy and security standards shall control.

- a. Authorized Functions. DE 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 APTCs 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, or Enrollees on insurance affordability programs and, if applicable, informing such individuals of eligibility for Medicaid or 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, and 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 DE Entity in connection with the FFEs, SBE-FPs, DE 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. Ability of Individuals to Limit Collection and Use. DE Entity agrees to provide the Consumer, Applicant, Qualified Individual, or Enrollee the opportunity to opt-in to have the DE Entity collect, create, disclose, access, maintain, store, and use their PII. DE Entity agrees to provide a mechanism through which a Consumer, Applicant, Qualified Individual, or Enrollee can limit the collection, creation, disclosure, access, maintenance, storage and use of their PII for the sole purpose of obtaining DE Entity's assistance in applying for a QHP, APTC or CSR eligibility, and for performing Authorized Functions specified in Section II.a of this Agreement.
 - c. Safeguards. DE Entity agrees to monitor, periodically assess, and update its security and privacy controls and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including Appendix B, "Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities," and Appendix E, "Security and Privacy Controls," and to timely inform the Exchanges of any material change in its administrative, technical, or operational environments, or that would alter CMS' understanding of DE Entity's network or system so that CMS may evaluate whether alterations of the privacy and security standards within this Agreement are necessary.
 - d. Downstream Entities. DE 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. DE Entity must require in writing all downstream and delegated entities to adhere to the terms of this Agreement.

- e. Critical Security and Privacy Controls. DE Entity shall implement a privacy and security framework that is aligned with National Institute for Standards and Technology (NIST) Special Publication 800-53, Revision 4 (NIST SP 800-53, Rev. 4) which includes the following critical controls (see Appendix E, "Security and Privacy Controls," for a comprehensive list of security and privacy controls):
 - 1. Email/Web Browser Protections – Including but not limited to assurance that transfer protocols are secure and limits the threat of communications being intercepted.
 - 2. Malware Protection – Including but not limited to protections against known threat vectors within the system's environment to mitigate damage/security breaches.
 - 3. Patch Management – Including but not limited to ensuring every client and server is up to date with the latest security patches throughout the environment.
 - 4. Vulnerability Management – Including but not limited to identifying, classifying, remediating, and mitigating vulnerabilities on a continual basis by conducting periodic vulnerability scans to identify weaknesses within an environment.
 - 5. Inventory of Software/Hardware – Including but not limited to maintaining an Inventory of hardware/software within the environment helps to identify vulnerable aspects left open to threat vectors without performing vulnerability scans and to have specific knowledge of what is within the system's environment.
 - 6. Account Management – Including but not limited to the determination of who/what has access to the system's environment and data and also maintain access controls to the system.
 - 7. Configuration Management – Including but not limited to defining the baseline configurations of the servers and endpoints of a system to mitigate threat factors that can be utilized to gain access to the system/data.
 - 8. Incident Response – Including but not limited to the ability to detect security events, investigate, and mitigate or limit the effects of those events.
 - 9. Governance and Privacy Compliance Program – Including but not limited to appointing a Responsible Official to develop and implement operational privacy compliance policies for information systems and databases.
 - 10. Privacy Impact/Risk Assessment – Including but not limited to appointing a Responsible Official to develop and implement a formal policy and procedures to assess the organizations risk posture.

11. Awareness and Training Program – Including but not limited to appointing a Responsible Official to develop and implement security and privacy education awareness program for all staff members and contractors.
 12. Data Retention and Destruction – Including but not limited to developing formal policy and procedures for data retention and destruction of PII.
 13. All employees, contractors, and other authorized users that send and receive data are guided by the following information system best practices:
 - i. Least Privilege: Only authorizing access to the minimal amount of resources required for a function;
 - ii. Separation of Duties: A basic control that prevents or detects errors and irregularities by assigning responsibility for initiating transactions, recording transactions and custody of assets to separate individuals; and
 - iii. Role-Based Security: Access controls to perform certain operations ('permissions') are assigned to specific roles.
 14. Modification to network or system – Any modifications to the DE Entity's network or system(s) that change in security posture shall be noted in writing and agreed upon and approved in writing by CMS or its designee.
 15. Current version of National Institute for Standards and Technology Special Publication 800-53 (NIST SP 800-53). Third party verification and documentation of the Non-Exchange Entity's compliance with the current NIST SP 800-53 that correspond to the critical controls listed above shall be accepted by CMS as documentation of compliance with those critical controls in Appendix E.
- f. Commitment to Protect Sensitive Information. The DE Entity shall not release, publish or disclose information 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 parties to support the management and operation of the interconnection.
 2. The overall sensitivity level of data or information that will be made available, exchanged, or passed two way only across the interconnection will be designated as MODERATE as determined by Federal Processing Standards (FIPS) Publication 199.
 3. DE Entity agrees to comply with all U.S. Federal laws and regulations regarding the handling of sensitive information – regardless of where the organization is located or where the data is stored and accessed.

4. DE Entity's Rules of Behavior must be at least as stringent as the HHS Rules of Behavior: <https://www.hhs.gov/ocio/policy/hhs-rob.html>
5. DE 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 the DE Entity shall be borne exclusively by the DE Entity.

III. 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 for the benefit year beginning January 1, 2019.
- b. Renewal. This Agreement may be renewed in the sole and absolute discretion of CMS for subsequent and consecutive one (1) year periods upon thirty (30) Days' advance written notice to DE Entity.

IV. 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. CMS may terminate this Agreement for cause upon sixty (60) Days' written notice to DE Entity if DE Entity materially breaches any term of this Agreement as determined in the sole but reasonable discretion of CMS, unless DE Entity commences curing such breach(es) within such 60-Day period to the reasonable satisfaction of CMS in the manner hereafter described in this subsection, and thereafter diligently prosecutes such cure to completion. A DE Entity's inability to perform due to a CMS error will not be considered a material breach. The 60-Day notice from CMS shall contain a description of the material breach and any suggested options for curing the breach(es), whereupon DE Entity shall have seven (7) Days from the date of the notice in which to propose a plan and a time frame to cure the material breach(es), which plan and time frame may be rejected, approved, or amended in CMS' sole but reasonable discretion. Notwithstanding the foregoing, DE Entity shall be considered in "Habitual Default" of this Agreement in the event that it has been served with a 60-Day notice under this subsection or an immediate suspension notice under Section IV.c. more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately terminate this Agreement upon notice to DE Entity without any further opportunity to cure or propose cure.
- c. Termination of Interconnection for Non-compliance. Non-compliance with the terms of this Agreement by DE Entity may lead to termination of the interconnection between the Parties. CMS may block the DE Entity's access to CMS systems if the DE 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. In accordance with section VII.k of this Agreement, CMS is authorized to audit the

security of DE Entity's network and systems periodically by requesting that DE Entity provide documentation of compliance with the privacy and security requirements in this Agreement. The DE Entity shall provide CMS access to its information technology resources impacted by this Agreement for the purposes of audits. CMS may suspend or terminate this Agreement if DE Entity does not comply with such a compliance review request within seven (7) business days. Further, notwithstanding Section IV.b. of this Agreement, CMS may immediately suspend the DE Entity's ability to transact information with the FFEs or SBE-FPs if CMS discovers circumstances that pose unacceptable or unmitigated risk to FFE operations or FFE information technology systems. If a DE Entity's ability to transact information with the FFEs or SBE-FPs is suspended, CMS will provide written notice to the DE Entity within two 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 the DE Entity's respective agreements with CMS (QHP Issuer Agreement and the Web-broker Agreement) or applicable program requirements. However, the termination of the DE Entity's other respective agreement(s) with CMS will result in termination of this Agreement and the ability of the DE Entity to use the Proxy DE Pathway as allowed by this Agreement.

V. Audit Requirements.

- a. Operational Readiness Review. In order to participate in the Proxy Direct Enrollment process, DE Entity must conduct an Operational Readiness Review (ORR) that verifies the DE Entity's Proxy DE Pathway, including its website and operations, complies with the terms of this Agreement, the DE Entity's respective agreement(s) with CMS, and applicable program requirements. The DE Entity must select an independent Auditor to conduct this ORR in accordance with this section V.

If the Auditor's ORR shows that DE Entity's Proxy DE Pathway does not fully comply with the terms of this Agreement, the DE Entity's respective agreement(s) with CMS, or any applicable program requirement, DE Entity may be conditionally approved to engage in Proxy Direct Enrollment if CMS, in its sole and absolute discretion, determines that the deficiencies present in the DE Entity's Proxy DE Pathway are sufficiently minor and can be sufficiently mitigated such that the DE Entity's participation in Proxy Direct Enrollment does not present unreasonable risk to the integrity of CMS programs and systems or the privacy and security of consumer information. DE Entities requesting conditional approval must submit documentation that at a minimum provides evidence of internal testing and audit of every critical control as provided in Appendix E. If a DE Entity participates in Proxy Direct Enrollment under such circumstances, DE Entity agrees to comply with any mitigation plans, schedules, or other requirements CMS identifies to ensure that DE Entity's Proxy Direct Enrollment Pathway is suitable for use by Exchange applicants, the terms of which are hereby incorporated into this Agreement as if fully set forth herein. DE Entity's failure to comply with any CMS mitigation plans, schedules, or other requirements may result in the immediate suspension of the DE Entity's ability to transact information with the FFEs or SBE-FPs in accordance with section IV.c. of

this Agreement and/or termination of this Agreement in accordance with section IV.b of this Agreement.

- b. Required Auditor Experience. DE Entity must select an Auditor with the following experience:
 - 1. Audit Experience. The Auditor must have experience conducting operational or security and privacy audits or similar services for federal, state, or private programs.
 - 2. Privacy and Security. The selected Auditor must be an independent party that has experience conducting privacy and security audits that encompass the operational, management and technical aspects of the DE's application using the standards and controls set forth by this Agreement, the DE Entity's respective agreement(s) with CMS, and applicable program requirements. Auditors must have experiences in performing penetration testing. Knowledge of HIPAA, NIST, HHS and CMS privacy and security standards is crucial to a successful and meaningful audit.
- c. Multiple Auditors. DE Entity may select multiple Auditors for conducting the ORR, but DE Entity must notify CMS of each Auditor, using the signature pages for this Agreement. If DE Entity's Auditor subcontracts to another Auditor(s), all Auditors and subcontractors will be considered downstream or delegated entities of the DE Entity pursuant to the DE Entity's respective agreement(s) with CMS and applicable program requirements. If a DE Entity uses multiple Auditors, the DE Entity must submit one findings report detailing the findings of its Auditors.
- d. Use of a Proxy DE Pathway Provided by Another Entity. DE Entity may use a Proxy DE Pathway provided by another entity (a Provider). Subject to requirements in this paragraph and Agreement, DE Entity may submit an ORR supplied by a Provider as its required ORR report submission to CMS, so long as the DE Entity attests that its implementation and use of the Provider's Proxy DE Pathway mirrors that described in the Provider's ORR and otherwise complies with all applicable regulations, operational requirements, and requirements of this Agreement.

If DE Entity will implement its own Proxy DE Pathway, only part of which will be comprised of a Provider's Proxy DE Pathway, DE Entity must conduct and submit an additional ORR report covering all functionalities and systems outside of the Provider's DE Pathway that evidences their compliance with applicable CMS regulations and this Agreement, as appropriate.

In all arrangements permitted under this paragraph, DE Entity is responsible for compliance with all requirements in regulations, guidance, and this Agreement by the Proxy DE Pathway it uses. Any provider supplying a Proxy DE Pathway to DE Entity will be a downstream or delegated entity of DE Entity. If applicable, DE Entity must identify its Provider on Appendix F of this Agreement.

- e. Auditor Training. All staff of an Auditor that are conducting audits pursuant to the terms of this Agreement must successfully complete CMS-mandated training, including completing CMS-specified training modules prior to conducting the ORR.
- f. Conflict of Interest. DE Entity must select an Auditor who 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. The DE Entity must disclose to IHHS any financial relationships between the Auditor, and individuals who own or are employed by the Auditor, and individuals who own or are employed by an Agent, Broker, or QHP Issuer for which the Auditor is conducting an ORR pursuant to 45 C.F.R. §§ 155.220(c)(3)(i)(K) or 156.1230(b)(2). DE Entity must complete the form in Appendix A if applicable.

VI. FFE Eligibility Application and Enrollment Requirements.

- a. Modifications to Application and Enrollment Pathway. DE Entity must notify CMS immediately if it intends to make any change to its Proxy DE Pathway that affects the information presented to the user regarding eligibility, the eligibility application, the eligibility determination, or enrollment processes. If DE Entity is responding to a CMS-initiated change to the streamlined eligibility application UI, DE Entity must provide confirmation to CMS that it has implemented the change.
- b. Maintenance of an Accurate Testing Environment. DE Entity must maintain a testing environment that accurately represents its production environment and Proxy DE Pathway including DE Entity's replication of FFE streamlined application UI. DE Entity must provide CMS with credentials to access this environment. If the testing environment is not appropriately firewalled from the production environment and PII, the testing environment must comply with the privacy and security controls detailed in this Agreement. DE Entity shall not submit PII to the FFE Testing Environments.
- c. Identify Proofing. DE Entity must conduct identity proofing for consumers entering the Proxy DE Pathway for enrollments. DE Entity must conduct identity proofing prior to submitting a consumer's application to the FFEs or SBE-FPs. If using the FFE's Remote Identity Proofing service, DE Entity must only use the service after confirming a consumer's eligibility for the Proxy DE Pathway and a consumer's intent to submit an FFE or SBE-FP Application. If DE Entity uses a different third-party identity proofing service, the service must be Federated Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS) approved, and DE Entity must be able to produce documentary evidence that each applicant has been successfully identity proofed.
- d. Accurate Reproduction of the FFE Streamlined Eligibility UI. DE Entity must replicate the FFE streamlined application UI content, structure and order, and logic for screener questions and processes as it appears on HealthCare.gov, unless CMS provides an approved alternative. This means that the screener questions must be in the same order, wording, and grouping logic as the questions on HealthCare.gov, unless CMS provides an approved alternative. DE Entity must implement the FFE streamlined application UI exactly as it appears on HealthCare.gov. This means that

DE Entity must replicate the HealthCare.gov question wording, answer choices (e.g., drop-down lists), structure and question order, question logic (i.e., connections between related questions), disclaimers (e.g., attestation disclaimer), and integrated help information including tool topics and boxes. CMS will not permit deviations from the FFE streamlined application UI, unless CMS requires specific deviations.

- e. Accurate Mapping. DE Entity's Proxy DE Pathway tools must accurately input consumer's responses to relevant FFE streamlined application UI fields. There can be no deviations from the eligibility application when automating the application on HealthCare.gov.
- f. Post-Eligibility Application Communications. DE Entity must provide consumers with the CMS-provided Eligibility Determination Notice (EDN) generated by the FFEs any time it submits or updates an application pursuant to requirements provided by CMS.
- g. Accurate Information About Exchanges and Consumer Communications. DE Entity must provide consumers using the Proxy DE Pathway with CMS-provided language informing and educating the consumer about the Exchanges, HealthCare.gov and Marketplace-branded communications a consumer may receive with important action items. CMS will provide additional details in the future.
- h. Post-Enrollment Support. DE Entity must notify consumers using the Proxy DE Pathway of data matching issues (DMIs), pre-enrollment special enrollment period (SEP) verification issues (SVIs), and clearly outline tax liability implications of APTC, including next steps for the consumer to submit documents to resolve DMIs and SVIs and pay premiums.

VII. 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 & Insurance Oversight
(CCIIO) Attn: Office of the Director
Room 739H
200 Independence Avenue, SW
Washington, DC 20201

If to DE Entity, to DE 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. DE 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. DE 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 DE Entity's respective agreement(s) with CMS. Notwithstanding any assignment of this Agreement or subcontracting of any responsibility hereunder, DE 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 FFM Web Services. DE Entity will only use a CMS-approved Proxy DE Pathway to facilitate enrollment through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix D.
- d. Survival. DE Entity's duty to protect and maintain the privacy and security of PII under this Agreement shall survive the expiration or termination of this Agreement.
- e. 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.
- f. Disclaimer of Joint Venture. Neither this Agreement nor the activities of DE 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 DE 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 PPACA and the regulations codified thereunder, including as codified at 45 C.F.R. part 155.
- g. 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.

- h. Compliance with Law. DE 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.
- i. 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. DE 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*.
- j. 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 DE 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. DE 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.
- k. Audit and Compliance Review. DE 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 DE Entity and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of DE Entity's compliance with the requirements of this Agreement and applicable program requirements upon reasonable notice to DE Entity, during DE Entity's regular business hours, and at DE Entity's regular business location. These audit and review rights include the right to audit DE Entity's compliance with and implementation of the privacy and security requirements under this Agreement, DE Entity's respective agreement(s) with CMS, and applicable program requirements. DE Entity further agrees to allow reasonable access to the information and facilities, including, but not limited to, DE 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. DE Entity is also responsible for ensuring cooperation by its

downstream and delegated entities, including DE 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 DE Entity does not comply with such a compliance review request within seven (7) business days.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

This "Agreement between DE 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:

FOR DE ENTITY

The undersigned is an authorized official of DE Entity who is authorized to represent and bind DE Entity for purposes of this Agreement.



Signature of Authorized Official of DE Entity

10/18/2017

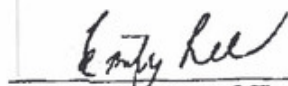
Date

David K. Francis, COO/CFO

Printed Name and Title of Authorized Official of DE Entity

eHealthInsurance Services, Inc.

DE Entity Name



Signature of Privacy Officer Attesting Compliance that DE Entity Systems Comply with the Critical Privacy and Security Controls under Section II.e of the Agreement

Emily Lee, Privacy Officer and Associate General Counsel

Printed Name and Title of Privacy Officer Attesting Compliance that DE Entity Systems Comply with the Critical Privacy and Security Controls under Section II.e of the Agreement

eHealthInsurance Services, Inc.

440 E. Middlefield Road

Mountain View, CA 94043

DE Entity Address

John Desser, SVP, Government Affairs/Public Policy

(202) 572-6907 Washington, D.C.

DE 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 C. Wu
-S

Digitally signed by Jeffrey C.
Wu -S
Date: 2017.10.27 17:56:16
-04'00'

10/27/2017

Jeff Wu
Associate Deputy Director for Policy Coordination
Center for Consumer Information & Insurance
Oversight
Centers for Medicare & Medicaid Services

Date

George C.
Hoffmann -S

Digitally signed by George C.
Hoffmann -S
Date: 2017.10.30 10:16:28
-04'00'

10/30/2017

George C. Hoffmann
Acting Chief Information Officer
Centers for Medicare & Medicaid Services

Date

APPENDIX A: CONFLICT OF INTEREST DISCLOSURE FORM

DE Entity must disclose to 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 an Agent, Broker, or QHP Issuer for which the Auditor(s) is conducting an operational readiness review pursuant to 45 C.F.R. §§ 155.220(c)(3)(i)(K) and/or 156.1230(b)(2). DE 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:

☒ DE Entity has no conflict of interest to report.

☐ DE 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 DE Entity

10/18/2017

Date

David K. Francis, COO/CFO

Printed Name and Title of Authorized Official of DE Entity

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

Statement of Applicability

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 2002 ("FISMA") (44 U.S.C. 3541), and 45 C.F.R. § 155.260. All capitalized terms used herein carry the meanings assigned in Appendix C, "Definitions." Any capitalized term that is not defined in Appendix C has the meaning provided in 45 C.F.R. § 155.20.

The standards and implementation specifications that are set forth in this Appendix B are consistent with the principles in 45 C.F.R. § 155.260(a)(1) through (a)(6).

The FFEs will enter into contractual agreements with all Non-Exchange Entities, including DE Entities that gain access to Personally Identifiable Information ("PII") exchanged with the FFEs and 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 B, 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 B has been incorporated, Non-Exchange Entities agree to comply with the standards and implementation specifications laid out in this document and the applicable standards, controls, and applicable implementation specifications within the privacy and security standards as established by the FFEs under 45 C.F.R. § 155.260(a)(3) and as applicable to Non-Exchange Entities under 45 C.F.R. § 155.260(b)(3) while performing the Authorized Functions outlined in their respective agreements.

NON-EXCHANGE ENTITY PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Non-Exchange Entities must meet the following privacy and security standards that correspond to 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, Non-Exchange Entities that maintain and/or store 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.*
 - a. Standard: Individual Access to PII. Non-Exchange Entities that maintain and/or store PII must implement policies and procedures that provide access to PII upon request.

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 their respective agreements with CMS.
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 the 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 them in determining their information or data needs, if such assistance is requested.
5. Subject to paragraphs (1)a.i.6 and 7 below, Non-Exchange Entities 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 their 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. Non-Exchange Entities 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, Non-Exchange Entities 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.

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, Non-Exchange Entities 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 FFEs, SBE-FPs, or Non-Exchange Entity obtains informed consent from such individuals.
 - 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, Non-Exchange Entities 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. 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. To the extent necessary to ensure the efficient operation of the Exchange;
 - ii. 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) above; and/or
 - iii. In accordance with the permissible functions outlined in the regulations and agreements between CMS and the Non-Exchange Entity.
- b. Standard: Non-discrimination. The 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. The 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. The 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 their SSN is relevant to verification of household income and family size.
 - 3. The 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 Entities should take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent such data is necessary for the Non-Exchange Entity's intended use of such data, and that such data has not been altered or destroyed in an unauthorized manner, thereby ensuring the confidentiality, integrity, and availability of PII.*

- a. Standard: Right to Amend, Correct, Substitute, or Delete PII. In keeping with the standards and implementation specifications used by the FFEs, Non-Exchange Entities must offer Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—an opportunity 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.
- 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. They may also be offered an opportunity to meet with the Responsible Official or their 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 their 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 their 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, Non-Exchange Entities that maintain and/or store 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 the Non-Exchange Entity. This includes confirmation of an individuals' 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 the 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 the 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 the Non-Exchange Entity, Non-Exchange Entities that maintain and/or store PII shall maintain an accounting of any and all 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, Non-Exchange Entities 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.*

- a. Standard: Reporting. The Non-Exchange Entity must implement Breach and Incident Handling procedures that are consistent with CMS' Incident and Breach Notification Procedures¹ 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.
 - 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

¹ Available at <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf>

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 C: 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) **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.
- (2) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 C.F.R. § 155.20.
- (3) **Agent or Broker** has the meaning set forth in 45 C.F.R. § 155.20.
- (4) **Applicant** has the meaning set forth in 45 C.F.R. § 155.20.
- (5) **Application Filer** has the meaning set forth in 45 C.F.R. § 155.20.
- (6) **Auditor** means a person or organization that meets the requirements set forth in this Agreement and contracts with an Agent, Broker, Web-broker, or issuer for the purposes of conducting an Operational Readiness Review in accordance with this Agreement and CMS-issued guidance.
- (7) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in the Agreement that incorporates this Appendix C.
- (8) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 C.F.R. § 155.227.
- (9) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for anything other than an authorized purpose.
- (10) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (CMS).
- (11) **CMS** means the Centers for Medicare & Medicaid Services.
- (12) **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.

- (13) **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.
- (14) **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 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.
- (15) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (QHP) 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 APTCs and CSRs, and/or completing enrollment in a QHP through the FFEs or SBE-FPs for individual market coverage.
- (16) **Cost-sharing Reductions (CSRs)** has the meaning set forth in 45 C.F.R. § 155.20.
- (17) **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 and providing information about eligibility and applying for APTCs and CSRs, Health Insurance Coverage, and enrollment processes in connection with the FFEs.
- (18) **Day or Days** means calendar days unless otherwise expressly indicated in the relevant provision of the Agreement that incorporates this Appendix C.
- (19) **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.
- (20) **Designated Security Official** means a contact person or office responsible for, 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.
- (21) **Direct Enrollment** means the process by which an Agent, Broker, 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), 156.265, and 156.1230.
- (22) **Direct Enrollment (DE) Entity** means a Non-Exchange Entity that performs Direct Enrollment under this Agreement.

- (23) **Enrollee** has the meaning set forth in 45 C.F.R. § 155.20.
- (24) **Enrollment Reconciliation** is the process set forth in 45 C.F.R. § 155.400(d).
- (25) **Exchange** has the meaning set forth in 45 C.F.R. § 155.20.
- (26) **Federally-facilitated Exchanges (FfEs)** means **Exchanges** (or **Marketplaces**) established by 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.
- (27) **FfE streamlined application user interface (UI)** means the application UI on HealthCare.gov available for Consumers with non-complex eligibility application responses determined by an initial set of eligibility questions for determining the complexity of an applicant's eligibility profile.
- (28) **Health Insurance Coverage** has the meaning set forth in 45 C.F.R. § 155.20.
- (29) **HHS** means the U.S. 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) **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.
- (32) **Information** means any communication or representation of knowledge, such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
- (33) **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 Qualified Health Plan through the Exchange with Cost-sharing Reductions established under section 1402 of the Patient Protection and Affordable Care Act.
- (34) **Issuer** has the meaning set forth in 45 C.F.R. § 144.103.
- (35) **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.
- (36) **OMB** means the Office of Management and Budget.
- (37) **Operational Readiness Review (ORR)** means an audit conducted under 45 C.F.R. §§ 155.220(c)(3)(i)(K) or 156.1230(b)(2) and includes the report submitted by a DE Entity detailing its compliance with CMS requirements and readiness to implement and use the Proxy DE Pathway.
- (38) **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.
- (39) **Provider** means an entity who provides a proxy DE pathway to a DE Entity.
- (40) **Proxy DE Pathway** means a DE process where a DE Entity collects eligibility information directly from consumers and uses a specific CMS-provided DE workflow with an automation tool to assist Consumers, Applicants, Qualified Individuals, and Enrollees in applying for APTCs and CSRs; applying for enrollment in QHPs offered through the FFEs or SBE-FPs; completing enrollment in QHPs offered through the FFEs or SBE-FPs; and providing Customer Service.
- (41) **Qualified Health Plan (QHP)** has the meaning set forth in 45 C.F.R. § 155.20.
- (42) **Qualified Health Plan (QHP) Issuer** has the meaning set forth in 45 C.F.R. § 155.20.
- (43) **Qualified Health Plan (QHP) Issuer Agreement** means the QHP Certification Agreement and Privacy and Security Agreement Between QHP Issuer and CMS.
- (44) **Qualified Individual** has the meaning set forth in 45 C.F.R. § 155.20.
- (45) **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.
- (46) **Security Control** means a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

- (47) **Special Enrollment Period (SEP)** has the meaning set forth in 45 C.F.R. § 155.20.
- (48) **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.
- (49) **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.
- (50) **State Partnership Exchange** means a type of FFE in which a State assumes responsibility for carrying out certain activities related to plan management, consumer assistance, or both.
- (51) **Subject Individual** means that individual to whom a SORN Record pertains.
- (52) **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.
- (53) **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.
- (54) **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 or voice print or a photograph, that is part of a System of Records.
- (55) **Web-broker** means an agent or broker who uses a non-Federally-facilitated Exchange Internet website to assist Consumers, Applicants, Qualified Individuals, and Enrollees in the QHP selection and enrollment process as described in 45 C.F.R. § 155.220(c).
- (56) **Web-broker Agreement** means the Agreement between Web-based Entity and CMS for the FFEs and SBE-FPs on the Federal Platform Individual Market.
- (57) **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.

**APPENDIX D: TECHNICAL AND TESTING STANDARDS
FOR USING THE PROXY DE PATHWAY**

- (1) CMS will provide DE Entity with a Direct Enrollment Proxy Operations Manual for the Proxy DE Pathway, the terms of which are specifically incorporated herein. DE Entity's use of the Proxy DE Pathway must comply with any standards detailed in the Operations Manual.
- (2) All proxy direct enrollments will occur with CMS-issued credentials by individuals responsible for proxy DE activities. Consistent with existing procedures, DE Entity may not create Exchange accounts or credentials on behalf of individual consumers.
- (3) The Proxy DE Pathway will be limited to simple cases currently served by the FFE streamlined application UI. Complex enrollments and terminations will not be supported. Furthermore, if, while testing the Proxy DE Pathway, a DE Entity identifies an eligibility scenario it cannot support in the Proxy DE Pathway, the DE Entity shall notify CMS that it cannot support this scenario in its ORR report. CMS reserves the right to review and approve a DE Entity's request to use the Proxy DE Pathway even if it cannot support all potential eligibility scenarios covered by the FFE streamlined Application UI. If DE Entity cannot support an eligibility scenario, DE Entity must provide alternative enrollment pathways to Consumers, Applicants, Qualified Individuals, and Enrollees, including, but not limited to, the DE double redirect process, the Exchanges, or the Marketplace call center.
- (4) CMS will not allow retries or bulk submissions due to the potential for degraded Exchange performance and availability which would impede the experience for all users.
- (5) Except as provided in Section V.d of this Agreement, DE Entity must not provide the capability for third-party agents or brokers or other downstream and delegated entities that are not or will not be a party to their own Proxy DE agreement with CMS to use its Proxy DE Pathway on the third party's own website or otherwise outside of the DE Entity's approved website and enrollment pathway identified by the DE Entity in its ORR report. Specifically, this prohibits embedding tools and programming techniques, such as iframe technical implementations, directing the consumer to third-party Agent or Broker websites.
- (6) DE Entity must implement tracking metrics on its Proxy DE Pathway to track Agent, Broker, Assister, or Consumer interactions with Consumer applications using a unique identifier for each individual, as well as an individual's interactions with the Exchange.
- (7) DE Entity must complete testing for each RIDP and Hub-related transaction it will implement, and 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 all applicable HIPAA compliance standards, or other CMS-approved standards, and to process data

transmitted by DE Entity to the Hub. The capability to submit these test transactions must be maintained by DE Entity throughout the term of this Agreement.

- (8) Transactions must be formatted in accordance with the Accredited Standards Committee Implementation Guides adopted under HIPAA, available at <http://store.x12.org/store/>, as applicable and appropriate for the type of transaction. The CMS Companion Guides for the transactions, which specify necessary situational data elements can be found at the following URL:
<https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/companion-guide-for-ffe-enrollment-transaction-v15.pdf> and <https://www.cms.gov/cciio/resources/regulations-and-guidance/index.html>.
- (9) DE 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.
- (10) DE 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 (1) and (2) above.
- (11) DE Entity agrees that CMS requires successful completion of an Operational Readiness Review (ORR) to the satisfaction of CMS, which must occur before DE Entity is able to submit any transactions using the specified Proxy DE Pathway provided by CMS to the FFE production system or at any time during the term of this Agreement. The ORR will assess DE Entity's compliance with CMS' regulatory requirements and with this Agreement, to include the critical 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.
- (12) All compliance testing (Operational, Management and Technical) of DE Entity will occur at a FIPS 199 MODERATE level due to the PII data contained within systems.
- (13) The ORR must detail the DE Entity's compliance with the requirements in CMS regulation and this Agreement as defined by the requirements and review standards detailed in Table 1.
- (14) To receive CMS approval to use the Proxy DE Pathway, DE Entity must submit all required documentation as detailed in Table 2 below.

Table 1. ORR Requirements

Eligibility Application	
Review Category	Audit Standards
Identity Proofing Implementation	<ul style="list-style-type: none"> ▪ <i>Requirement:</i> DE Entity must conduct identity proofing for consumers entering the Proxy DE Pathway for enrollments. DE Entity must conduct identity proofing prior to submitting a Consumer's application to the FFEs or SBE-FPs. CMS will make the FFE Remote Identity Proofing (RIDP) service available to DE entities. A DE entity does not need to use third-party identity proofing if it already uses the approved FFE RIDP service. If the DE entity uses the FFE RIDP service, it must use the RIDP service only after confirming the consumer will submit an application to the FFE or SBE-FP, but prior to submitting the application. If DE Entity uses a third-party identity proofing service, the service must be FICAM TFS approved, and DE 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 this Agreement. Applicants do not need to be ID proofed on subsequent interactions with the DE Entity if the Applicant creates an account (i.e., username and password) on the DE Entity site. ▪ <i>Review Standard:</i> If the DE Entity uses a third-party identity proofing service, the Auditor must evaluate and certify that the identity proofing service is FICAM TFS approved and that the DE Entity has implemented the service correctly. If the DE Entity uses the FFE RIDP service, the Auditor must verify the DE Entity has implemented the service correctly.
Accurate Implementation of the Streamlined Application UI Screener Questions & Processes	<ul style="list-style-type: none"> ▪ <i>Requirement:</i> DE Entity must implement the FFE streamlined application UI screener questions exactly as they appear on HealthCare.gov. This means the questions must be in the same order as the existing questions with the same wording and grouping logic unless CMS provides an approved alternative. For plan year 2018, CMS is not allowing DE entities to use the Proxy DE Pathway for enrollments that require the FFE classic application (i.e., more complex situations, such as a multi-tax-filer household). ▪ <i>Review Standard:</i> Auditors must document that the DE Entity has accurately reproduced the eligibility questions and structured the questions with the same application flow as the FFE streamlined application UI, unless CMS provides an approved alternative. In such a case, Auditors must document that the DE Entity has accurately reproduced the eligibility questions and structured the questions consistent with the CMS-approved alternative method. The Auditor must also verify that if a Consumer responds to a screener question in a way that would direct the Consumer to the FFE classic application, the DE Entity provides an alternative enrollment pathway that does not use the Proxy DE Pathway.
Accurate Reproduction of the FFE Streamlined Application UI	<ul style="list-style-type: none"> ▪ <i>Requirement:</i> DE Entity must implement the FFE streamlined application UI exactly as it appears on HealthCare.gov. This includes identical question wording, answer choices (e.g., drop-down lists), structure and question order, question logic (i.e., connections between related questions), disclaimers (e.g., attestation disclaimer), and integrated help information including tool tips and boxes. CMS will not permit any deviations from the FFE streamlined application UI unless CMS requires specific deviations. Incorrect question and answer choices may yield incorrect eligibility determinations. ▪ <i>Review Standard:</i> Auditors must review and document that the FFE streamlined application UI content, structure, and logic has been accurately implemented on the DE entity's website(s) and complies with the above standards. Auditors must review for eligibility scenarios provided by CMS to verify the DE entity has mapped all of the FFE streamlined application UI. For example, the FFE streamlined application UI's structure and questions change if consumers or agents and brokers indicate dependents, or certain income options on the eligibility application.

Review Category	Audit Standards
Accurate Mapping of Eligibility Responses to the FFE Eligibility Application	<ul style="list-style-type: none"> ▪ Requirement: DE Entity's Proxy DE Pathway tools must accurately input consumer's responses to relevant FFE streamlined application UI fields. There can be no deviations from the FFE streamlined application UI when automating the application on HealthCare.gov. ▪ Review Standard: Auditors must review the application mapping to verify the DE Entity's automation tool is correctly completing the FFE streamlined application UI on HealthCare.gov. The Auditor should customize the review standard to the DE Entity's implementation of the automation tool.
Post-eligibility Application Communications	<ul style="list-style-type: none"> ▪ Requirement: DE Entity must provide consumers with the CMS-provided EDN generated by the FFEs any time it submits or updates an application pursuant to requirements provided by CMS. ▪ Review Standard: Auditors must verify that the DE Entity's Proxy DE Pathway notifies consumers of their eligibility results prior to QHP submission including submitting a Change in Circumstance (CiC) on the pathway. For example, if a consumer's APTC or CSR eligibility changes, the DE entity must notify the consumer of the change and allow the consumer to modify his or her QHP selection or APTC allocation accordingly. DE Entity must have a process for providing consumers with an EDN in the Proxy DE Pathway. DE Entity must share required eligibility information that will be specified by CMS in subsequent guidance.
Accurate Information About the Exchange and Consumer Communications	<ul style="list-style-type: none"> ▪ Requirement: DE Entity must provide consumers with CMS provided language informing and educating the consumer about the Exchanges and HealthCare.gov and Marketplace-branded communications a consumer may receive with important action items. CMS will define these requirements in guidance. ▪ Review Standard: Auditors must verify that the DE Entity's Proxy DE Pathway includes all required language, content, and disclaimers provided by CMS in accordance with the requirements stated in guidance.
Documentation of Interactions with Consumer Applications or the Exchanges	<ul style="list-style-type: none"> ▪ Requirement: DE Entity must implement tracking metrics on its Proxy DE Pathway to track Agent, Broker, Assister, or Consumer interactions with Consumer applications using a unique identifier for each individual, as well as an individual's interactions with the Exchanges. ▪ Review Standard: Auditors must verify the DE Entity's process for determining and tracking when an individual, Agent, Broker, Assister, or Consumer has interacted with a Consumer application or actions utilizing the Proxy DE Pathway.

Review Category	Audit Standards
Eligibility Results Testing	<ul style="list-style-type: none"> ▪ Requirement: DE Entity must submit accurate applications through the Proxy DE Pathway that result in accurate and consistent eligibility determinations for a variety of consumer eligibility scenarios. The ORR must include testing results either in the existing FFE test environment or the final implementation of the Proxy DE Pathway, depending on the timing of the ORR submission. If the ORR includes testing results using the existing FFE test environment, the DE Entity must submit an additional attestation after the final implementation of the Proxy DE Pathway has been released in an FFE testing environment. CMS will provide a resource on CMS zONE containing the eligibility scenarios for Auditors to test on the Proxy DE Pathway or FFE testing environment. ▪ Review Standard: Auditors must complete a series of test eligibility scenarios using the DE Entity's Proxy DE Pathway implementation. For example, these scenarios may include Medicaid and CHIP eligibility, different combinations of APTC and CSR, and non-streamlined application UI scenarios (i.e., scenarios that would require the FFE classic application). 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 DE Entity and Auditor to submit FFE Application IDs, eligibility response XMLs, and EDNs for each test scenario.

Privacy and Security Requirements

Review Category	Audit Standards
Privacy and Security Compliance	<ul style="list-style-type: none"> ▪ Requirement: DE Entity must comply with the privacy and security standards in both their respective agreements with CMS and this Agreement. DE Entity must also comply with HealthCare.gov data collection requirements as provided by CMS. ▪ Review Standard: Auditors must complete a privacy and security risk assessment to review and certify that the DE Entity has implemented processes sufficient to meet the regulatory privacy and security requirements. Auditors must verify that the DE Entity's website complies with the privacy and security standards detailed in this Agreement and that the website is consistent with third-party data collection tools and standards to be defined by CMS in subsequent guidance; CMS regulations; and subsequent guidance, technical, and training documents.

Table 2. Required Documentation

Document	Description	Submission Requirements
Intent to Participate	<ul style="list-style-type: none"> ▪ QHP issuers and web-brokers must notify CMS if they intend to apply to use the Proxy DE Pathway for plan year 2018, beginning with the 2018 OEP. 	<ul style="list-style-type: none"> ▪ DE Entity should email directenrollment@cms.hhs.gov Subject line should state: "DE Proxy: Intent"
DE Proxy Agreement	<ul style="list-style-type: none"> ▪ DE Entity must submit this Agreement to use the Proxy DE Pathway. The Agreement must identify the DE Entity's selected Auditor. ▪ CMS will countersign this Agreement after CMS has reviewed and approved the ORR findings report and the eligibility results attestation. 	<ul style="list-style-type: none"> ▪ DE Entity should submit the Agreement via email to directenrollment@cms.hhs.gov ▪ Subject line should state: "DE Proxy: Agreement"

Document	Description	Submission Requirements
Detailed ORR Findings Report (includes the privacy & security risk assessment report)	Audit report topics: <ul style="list-style-type: none"> ▪ Executive Summary <ul style="list-style-type: none"> – Scope of audit – Summary of methodology – General conclusions with respect to compliance ▪ Methodology ▪ Detailed findings, such as: <ul style="list-style-type: none"> – Eligibility application screener and application implementation and mapping results – RIDP implementation or other identity-proofing mechanism – Eligibility results testing – Privacy and security standards ▪ Risks and Recommendations <ul style="list-style-type: none"> – The report must include a mitigation strategy plan, developed by the Auditor and DE Entity, based on any identified risks. – <u>Privacy and security risk assessment report and mitigation strategies:</u> Auditors must assign a risk level to all privacy and security findings. HIGH risk findings must be remediated prior to use of the Proxy DE Pathway. Findings assigned lower risk must be presented with mitigation strategies for CMS review. – Attestation that the DE Entity is compliant with the applicable regulations and agreement provisions based on the ORR findings 	<ul style="list-style-type: none"> ▪ Format: PDF ▪ Page limit: 10 pages ▪ DE Entity should submit its ORR Findings Report via email to directenrollment@cms.hhs.gov ▪ Subject line should state: "DE Proxy: Audit Report"
Eligibility Results Submission & Attestation (if applicable)	<ul style="list-style-type: none"> ▪ DE Entity must attest that their Proxy DE Pathway generates accurate eligibility results. DE Entity may need to submit the results twice depending on the timeline of their ORR submission. ▪ CMS will not countersign this Agreement until receiving this attestation. Once CMS receives the eligibility results and attestation submission and verifies its accuracy and completeness, CMS will countersign this Agreement. 	<ul style="list-style-type: none"> ▪ DE Entity should submit this attestation via email to directenrollment@cms.hhs.gov. ▪ The attestation must include FFE Application IDs, eligibility response XMLs, and EDNs for each test scenario. Subject line should state "DE Proxy: Eligibility Results"

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

APPENDIX E: SECURITY AND PRIVACY CONTROLS

The table provides the critical controls with which the DE Entity must comply. The controls are a subset of NIST SP 800-53, Rev. 4 security and privacy controls.² The table provides a cross walk to HIPAA Security Rules.

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
Access Control (AC)	AC-1	Access Control Policy and Procedures	164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	AC-2	Account Management	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(b), 164.312(d), 164.312(e), 164.312(e)(2)(i)

² NIST Special Publication 800-53 (Rev. 4) is available at the following link: <https://nvd.nist.gov/800-53/Rev4>

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	AC-2(3)	Disable Inactive Accounts	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(b), 164.312(d), 164.312(e), 164.312(e)(2)(i)
	AC-2(4)	Automated Audit Actions	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(b), 164.312(d), 164.312(e), 164.312(e)(2)(i)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	AC-2(10)	Shared / Group Account Credential Termination	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(b), 164.312(d), 164.312(e), 164.312(e)(2)(i)
	AC-3	Access Enforcement	164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)
	AC-3(9)	Access Enforcement – Controlled Release	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(b), 164.312(d), 164.312(e), 164.312(e)(2)(i)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	AC-4	Information Flow Enforcement	164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(d), 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)
	AC-5	Separation of Duties	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii) 164.312(e)
	AC-6	Least Privilege	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(e)
	AC-6(5)	Privileged Accounts	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(e)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	AC-6(9)	Auditing Use of Privileged Functions	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(e)
	AC-7	Unsuccessful Logon Attempts	
	AC-8	System Use Notification	
	AC-11	Session Lock	
	AC-12	Session Termination	
	AC-14	Permitted Actions Without Identification or Authentication	
	AC-17	Remote Access	164.308(a)(1)(ii)(D), 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(e), 164.312(e)(1), 164.312(e)(2)(ii)
	AC-18	Wireless Access	164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(b), 164.312(e)
	AC-20	Use of External Information Systems	164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.308(b), 164.308(b)(1), 164.308(b)(3), 164.312(e)(1), 164.312(e)(2)(ii), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	AC-20(1)	Limits on Authorized Use	164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.308(b), 164.308(b)(1), 164.308(b)(3), 164.312(e)(1), 164.312(e)(2)(ii), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)
	AC-20(2)	Portable Storage Devices	164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.308(b), 164.308(b)(1), 164.308(b)(3), 164.312(e)(1), 164.312(e)(2)(ii), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2)
	AC-21	Information Sharing	164.308(a)(6)(ii)
	AT-2	Security Awareness Training	164.308(a)(5)
Awareness and Training (AT)	AT-2(2)	Insider Threat	164.308(a)(5)
Audit and Accountability (AU)	AU-2	Audit Events	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)
	AU-6	Audit Review, Analysis, and Reporting	164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(6)(i), 164.308(a)(6)(ii), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
	AU-9	Protection of Audit Information	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)
	AU-11	Audit Record Retention	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.310(a)(2)(iv), 164.310(d)(2)(iii), 164.312(b)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
Security Assessment and Authorization (CA)	CA-2	Security Assessments	164.308(a)(6)(ii), 164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(a)(2)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)
	CA-2(1)	Independent Assessors	164.308(a)(6)(ii), 164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(a)(2)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)
	CA-3	System Interconnections	164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d), 164.312(b)
	CA-5	Plan of Action and Milestones	
	CA-6	Security Authorization	

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	CA-7	Continuous Monitoring	164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(b), 164.312(d), 164.312(e), 164.312(e)(2)(i), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.314(b)(2)(i), 164.316(b)(2)(iii)
	CA-9	Internal System Connections	164.308(a)(1)(ii)(A), 164.308(a)(3)(ii)(A), 164.308(a)(8), 164.310(d)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
Configuration Management (CM)	CM-2	Baseline Configuration	164.308(a)(4)* 164.308(a)(7)(i), 164.308(a)(7)(ii), 164.308(a)(8), 164.308(a)(1)(ii)(D), 164.312(b) *Additionally, organizations should consider the HIPAA Privacy Rule "minimum necessary" standard, 45 C.F.R. § 164.502(b), when determining the level of access that is appropriate for development and testing staff.
	CM-3	Configuration Change Control	164.308(a)(7)(i), 164.308(a)(7)(ii), 164.308(a)(8), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.312(e)(2)(i), 164.314(b)(2)(i)
	CM-4	Security Impact Analysis	164.308(a)(7)(i), 164.308(a)(7)(ii), 164.308(a)(8)
	CM-6	Configuration Settings	164.308(a)(7)(i), 164.308(a)(7)(ii), 164.308(a)(8)
	CM-7	Least Functionality	164.308(a)(7)(i), 164.308(a)(7)(ii), 164.308(a)(8), 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	CM-8	Information System Component Inventory	164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)
	CM-11	User-Installed Software	164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)
	IA-2	Identification and Authentication (Organizational Users)	164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
Identification and Authentication (IA)	IA-4	Identifier Management	164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
	IA-5	Authenticator Management	164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	IA-5(1)	Password-Based Authentication	164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
	IA-5(15)	FICAM-Approved Products and Services	164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
	IA-8	Identification and Authentication (Non-Organizational Users)	164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
Incident Response (IR)	IR-1	Incident Response Policy and Procedures	164.306, 164.308, 164.310, 164.312, 164.314, 164.316

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	IR-4	Incident Handling	164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(7), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(2)(i), 164.310(d)(2)(iii), 164.312(a)(2)(ii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)
	IR-5	Incident Monitoring	164.308(a)(1)(i), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii), 164.308(a)(8), 164.310(d)(2)(iii), 164.312(b), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
	IR-6	Incident Reporting	164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii)
Maintenance (MA)	MA-2	Controlled Maintenance	164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)
	MA-5	Maintenance Personnel	164.308(a)(3)(ii)(A), 164.310(a)(2)(iv)
Media Protection (MP)	MP-2	Media Access	164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)
	MP-3	Media Marking	

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	MP-6	Media Sanitization	164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2), 164.310(d)(2)(i), 164.310(d)(2)(ii)
Physical and Environmental Protection (PE)	PE-2	Physical Access Authorizations	164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)
	PE-3	Physical Access Control	164.306(e), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)
	PE-18	Location of Information System Components	164.308(a)(7)(i), 164.308(a)(7)(ii)(C), 164.310, 164.316(b)(2)(iii)
Planning (PL)	PL-2	System Security Plan	164.306(e), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii)
	PL-4	Rules of Behavior	

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
Personnel Security (PS)	PS-3	Personnel Screening	164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(3), 164.310(b), 164.310(c), 164.312(a), 164.312(e)
	PS-6	Access Agreements	164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(3), 164.310(b), 164.310(c), 164.312(a), 164.312(e)
	PS-7	Third-Party Personnel Security	164.308(a)(1)(i), 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b), 164.308(b)(1), 164.314, 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii), 164.316
Risk Assessment (RA)	RA-3	Risk Assessment	164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(6), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316, 164.316(a), 164.316(b)(2)(iii)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	RA-5	Vulnerability Scanning	164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)
	RA-5(1)	Update Tool Capability	164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)
	RA-5(2)	Update by Frequency/Prior to New Scan/When Identified	164.306(e), 164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.314(a)(2)(i)(C), 164.314(a)(2)(iii), 164.316(b)(2)(iii)
System and Services Acquisition (SA)	SA-3 SA-4	System Development Life Cycle Acquisition Process	164.308(a)(1)(i) 164.308(a)(1)(i) 164.308(a)(1)(ii)(D)
	SA-5	Information System Documentation	164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	SA-10	Developer Configuration Management	164.308(a)(1)(i), 164.308(a)(7)(i), 164.308(a)(7)(ii), 164.308(a)(8)
	SA-11	Developer Security Testing and Evaluation	164.308(a)(1)(i), 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)
	SA-22	Unsupported System Components	
System and Communications Protection (SC)	SC-8	Transmission Confidentiality and Integrity	164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.310(b), 164.308(b)(1), 164.308(b)(2), 164.310(c), 164.312(a), 164.312(e), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)
	SC-12	Cryptographic Key Establishment and Management	
	SC-23	Session Authenticity	
	SC-28	Protection of Information at Rest	164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)
System and Information Integrity (SI)	SI-3	Malicious Code Protection	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.306(e)
	SI-3(2)	Automatic Updates	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.306(e)

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
	SI-5	Security Alerts, Advisories, and Directives	164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(D), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(6), 164.308(a)(8), 164.310(a)(1), 164.310(a)(2)(iii), 164.312(a)(1), 164.312(c), 164.312(e), 164.314, 164.316, 164.316(b)(2)(iii)
	SI-7	Software, Firmware, and Information Integrity	164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)
	SI-10	Information Input Validation	
	SI-11	Error Handling	
Authority and Purpose (AP)	AP-1	Authority to Collect	164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	AP-2	Purpose Specification	
Accountability, Audit, and Risk Management (AR)	AR-1	Governance and Privacy Program	164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	AR-2	Privacy Impact and Privacy Program	
	AR-5	Privacy Awareness and Training	
	AR-8	Accounting of Disclosures	
Data Quality and Integrity (DI)	DI-1	Data Quality	164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	DI-1(1)	Validate PII	164.306, 164.308, 164.310, 164.312, 164.314, 164.316

Security/Privacy Control	Control #	Security/Privacy Control Name	Corresponding HIPAA Security Rule 45 C.F.R.
Data Minimization and Retention (DM)	DM-1	Minimization of Personally Identifiable	164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	DM-2	Data Retention and Disposal	
	DM-3	Minimization of PII Used in Testing, Training, and Research	
	DM-3 (1)	Minimization of PII Used in Testing, Training, and Research/Risk Minimization Techniques	
Individual Participation and Redress (IP)	IP-1	Consent	164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	IP-2	Individual Access	
	IP-3	Redress	
	IP-4	Complaint Management	
Security (SE)	SE-1	Inventory of Personally Identifiable Information	164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	SE-2	Privacy Incident Response	
Transparency (TR)	TR-1	Privacy Notice	164.306, 164.308, 164.310, 164.312, 164.314, 164.316
	TR-2	System of Records Notices and Privacy Act Statements	
	TR-3	Dissemination of Privacy Program Information	
Use Limitation (UL)	UL-1	Internal Use	164.306, 164.308, 164.310, 164.312, 164.314, 164.316

APPENDIX F: AUDITOR IDENTIFICATION

The DE Entity agrees to identify, in Part I below, the Auditors selected to complete the Operational Readiness Review (ORR), in addition to any subcontractors of the Auditor, if applicable. In the case of multiple Auditors, please indicate what role each Auditor will serve in completing the ORR. Include additional sheets, if necessary.

If the DE Entity is using an ORR provided by another entity, pursuant to Section V.d, complete Part II below. If necessary, pursuant to Section V.d, complete Part I to indicate any additional independent audits conducted to verify compliance of the DE Entity's implementation of the Proxy DE Pathway.

TO BE FILLED OUT BY DE ENTITY

I. Complete These Rows if the DE Entity Is Conducting an Audit

Printed Name and Title of Authorized Official of Auditor 1	Daniel Powers, Senior Consultant
Auditor 1 Name	A-LIGN CPA, LLC
Auditor 1 Address	Rivergate Tower, 400 N. Ashley Drive, Suite 1325, Tampa, Florida 33602
Auditor 1 Contact Number	(909) 297-6514
Subcontractor Name & Information (if applicable)	
Audit Role (if applicable)	
Printed Name and Title of Authorized Official of Auditor 2	
Auditor 2 Name	
Auditor 2 Address	
Subcontractor Name & Information (if applicable)	
Audit Role (if applicable)	

II. Complete These Rows if DE Entity's Proxy DE Pathway Is Provided by Another Entity

Name of Entity Providing Proxy DE Pathway	
Address of Entity Providing Proxy DE Pathway	
Printed Name and Title of Authorized Official of Entity Providing the Proxy DE Pathway	
Contact Information for Authorized Official of Entity Providing the Proxy DE Pathway	
Is the Entity Providing an ORR Report for the Proxy DE Pathway?	

