AGREEMENT BETWEEN THE CENTERS FOR MEDICARE & MEDICAID SERVICES AND CERTIFIED APPLICATION COUNSELOR DESIGNATED ORGANIZATION IN A STATE IN WHICH A FEDERALLY-FACILITATED EXCHANGE IS OPERATING

THIS AGREEMENT ("Agreement") is entered into by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES ("CMS"), as the Party (as defined below) responsible for the management and oversight of the Federally-facilitated Exchanges ("FFEs"), and _____ _____[insert name and designation number of organization], an organization that has been designated by CMS as a Certified Application Counselor Designated Organization (hereinafter referred to as "CDO") in _____[insert name of applicable FFE state(s) in which organization is designated], a State/States in which an FFE is operating. CMS and CDO are hereinafter sometimes referred to as "Party" or, collectively, as the "Parties."

WHEREAS:

1. Pursuant to 45 CFR 155.225(b), to facilitate the operation of the FFE, CMS may designate an organization to certify its staff members or volunteers to act as Certified Application Counselors (CACs).

2. Pursuant to 45 CFR 155.225(c), CACs are expected to provide the following services to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s):
    a. Provide information about the full range of Qualified Health Plan (QHP) options and Insurance Affordability Programs for which these persons are eligible;
    b. Assist with applications for coverage in a QHP through the FFE and for Insurance Affordability Programs; and
    c. Help to facilitate enrollment in QHPs and Insurance Affordability Programs.

3. Pursuant to 45 CFR 155.225(b)(1)(i), to be designated as a CDO, an organization must enter into an agreement with the Exchange to comply with the standards and requirements of 45 CFR 155.225, including but not limited to 45 CFR 155.225(d)(3)-(5).

4. To facilitate the operation of the FFE, CMS has determined that it would be beneficial to permit CDO, and the staff members and volunteers CDO certifies as CACs, to create, collect, disclose, access, maintain, store, or use Personally Identifiable Information ("PII") from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, Qualified Employers, or their legal representative(s) or Authorized Representative(s), to the extent that these activities are necessary to carry out the Authorized Functions that the Affordable Care Act ("ACA"), implementing regulations, and this Agreement permit.

5. CDO has determined that it would be beneficial to permit the staff members and volunteers it certifies as CACs to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, Qualified Employees, Qualified Employers, and Enrollees, or their legal representative(s) or Authorized Representative(s), in order to perform the Authorized Functions described in Section III.2 of this Agreement.

6. 45 CFR 155.260(b) provides that an Exchange must require the same or more stringent privacy and security standards as are established and implemented for the Exchange under 45 CFR 155.260(a), as a condition of contract or agreement with Non-Exchange Entities, and CDO is a Non-Exchange Entity.

7. CMS, in the administration of the FFEs, has adopted privacy and security standards concerning PII, as set forth in the attached Appendix A, "Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities," which is hereby incorporated by reference. Compliance with this Agreement satisfies the requirement under 45 CFR 155.225(d)(3) to comply with applicable authentication and data security standards.

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

I. DEFINITIONS. Capitalized terms not otherwise specifically defined herein shall have the meaning set forth in the attached Appendix B, "Definitions," and/or in 45 CFR 155.20, which definitions are hereby incorporated by reference.

II. OBLIGATIONS AND CONDITIONS. To carry out the functions authorized by 45 CFR 155.225, and as a condition of its designation as a CDO by the FFE, CDO agrees to:

1. Certify one or more individual staff members and/or volunteers of the CDO to serve as CACs who are authorized to facilitate the efficient operation of one or more specific FFEs. Such certification shall include the assignment of a unique CAC identification number, as described in Section II.3 of this Agreement, and the issuance of a CAC Certificate to each individual staff member or volunteer that is certified by the CDO to serve as a CAC. CAC Certificates must include the staff member or volunteer's name and unique CAC identification number;

2. Prior to certifying any staff member or volunteer to serve as a CAC, do all of the following:

    a. Ensure that each such staff member or volunteer seeking certification as a CAC completes CMS-approved training regarding QHP options, Insurance Affordability Programs, eligibility, and benefits rules and regulations governing all Insurance Affordability Programs operated in the state, as implemented in the state, and completes and achieves a passing score on all CMS-approved certification examinations, prior to functioning as a CAC;

b. Require each such staff member or volunteer seeking certification as a CAC to enter into a written, signed agreement with the CDO that requires the individual staff member or volunteer seeking certification as a CAC to:

i. Register for CMS-approved training using his or her unique CAC identification number and the name that will appear on both his or her CAC Certificate and Training Certificate, complete the training and examination requirements described in Section II.2.a of this Agreement, and provide proof in the form of his or her Training Certificate to the CDO that he or she has fulfilled the training and examination requirements;

ii. Disclose to the CDO and to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s), any relationships the CAC has with QHPs or Insurance Affordability Programs, or other potential conflicts of interest, and, if the CDO elects to comply with Section II.5 of this Agreement by requiring CACs to do so, disclose to any Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) any potential conflicts of interest of the CDO;

iii. Comply with the FFE's Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities, which was drafted in conformance with 45 CFR 155.260, and applicable authentication and data security standards, through provisions that impose the same duties and obligations as those imposed on CDO by Section III and Appendix A of this Agreement;

iv. Act in the best interest of any Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, or Qualified Employers that he or she assists;

v. Either directly or through an appropriate referral to a Navigator or non-Navigator assistance personnel authorized under 45 CFR §§ 155.205(d) and (e) or 155.210, or to the Exchange call center authorized under 45 CFR § 155.205(a), provide information in a manner that is accessible to individuals with disabilities, as defined by the Americans with Disabilities Act, as amended, 42 USC § 12101, et seq. and section 504 of the Rehabilitation Act, as amended, 29 USC § 794;

vi. Inform Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) of the functions and responsibilities of Certified Application Counselors. CDO and its staff

members and/or volunteers may use the model form provided by CMS and appended hereto and referred to as Appendix E to fulfill this requirement;

vii. Prior to creating, collecting, disclosing, accessing, maintaining, storing, or using any PII of Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, Qualified Employers, and/or their legal representative(s) or Authorized Representative(s), obtain the authorization required by 45 CFR 155.225(f) and section II.8 of this Agreement (hereinafter referred to as "authorization") to: create, collect, disclose, access, maintain, store, and use PII of such person(s) to carry out the Authorized Functions listed at Section III.2 of this Agreement. This authorization may be obtained either directly from the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and/or Qualified Employer, or through such person(s)' legal representative(s) or Authorized Representative(s). CDO and its staff members and/or volunteers may use the model form provided by CMS and appended hereto and referred to as Appendix E to fulfill this requirement. This authorization is separate and distinct both from any authorization obtained pursuant to section III.7 of this agreement and from the informed consent referenced in Appendix A at 3(a);

viii. Maintain a record of the authorization provided under Section II.2.b.vii;

ix. Permit the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and Qualified Employer, and/or these individuals' legal representative(s) or Authorized Representative(s) to revoke the authorization described in Section II.2.b.vii at any time;

x. Not impose any charge or fee on Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) for application or other assistance related to the Exchange;

xi. Prominently display to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s), the CAC Certificate provided by the CDO evidencing the staff member's or volunteer's certification as a CAC each time the staff member or volunteer assists any Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s);

xii. Provide information to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) about

the full range of QHP options and Insurance Affordability Programs for which they are eligible;

xiii. Assist Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) in applying for coverage in a QHP through the Marketplace and for Insurance Affordability Programs;

xiv. Help to facilitate enrollment of eligible Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers in QHPs and Insurance Affordability Programs, either directly or through these individuals' legal representative(s) or Authorized Representative(s);

xv. Provide his or her unique CAC identification number to any Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and Qualified Employer, and/or these individuals' legal representative(s) or Authorized Representative(s) assisted by the staff member or volunteer, and include his or her unique CAC identification number on any application that is fully or partially completed in connection with the staff member or volunteer's assistance for that individual;

xvi. Upon termination or nonrenewal of CAC's agreement with CDO, or withdrawal of designation from CDO or withdrawal of certification from CAC, immediately cease holding himself or herself out as a CAC to any Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and Qualified Employer, and/or these individuals' legal representative(s) or Authorized Representative(s), and immediately cease providing certified application counselor CAC services to the public;

xvii. Not sell or otherwise transfer information provided by Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) to any person or entity other than such actions as are specifically permitted by this Agreement; and

xviii. Not collect or otherwise maintain information provided by Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s), except as specifically provided for in this Agreement.

3. Maintain a registration process and method to track the performance of CACs. This tracking method shall include assigning a unique CAC identification number to each staff member or volunteer certified by the CDO to serve as a CAC, which shall consist of an identification number that CMS assigns the CDO and that identifies the CDO, followed

by the unique identification number assigned to each individual staff member or volunteer by the CDO.

4. Upon request, provide to CMS the names and CAC identification numbers assigned by the CDO of all staff members and volunteers that have been certified by the CDO to serve as CACs;

5. Establish procedures to directly, or, if the CDO so elects, through its CACs, disclose all potential conflicts of interest of the CDO to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) prior to providing assistance to any such individuals, including any relationships the CDO has with QHPs or Insurance Affordability Programs, or other potential conflicts of interest;

6. Act in the best interests of the Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers assisted by the CDO and by the staff members and volunteers it has certified as CACs;

7. Either directly or through an appropriate referral to a Navigator or non-Navigator assistance personnel authorized under 45 CFR §§ 155.205(d) and (e) or 155.210, or to the Exchange call center authorized under 45 CFR § 155.205(a), provide information in a manner that is accessible to individuals with disabilities, as defined by the Americans with Disabilities Act, as amended, 42 USC § 12101, et seq. and section 504 of the Rehabilitation Act, as amended, 29 USC § 794;

8. Establish procedures to ensure, pursuant to 45 CFR 155.225(f), that Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s):

    a. Are informed of the functions and responsibilities of CACs. CDO and its staff members and/or volunteers may use the model form provided by CMS and appended hereto and referred to as Appendix E to fulfill this requirement;

    b. Provide authorization, before CDO or any of CDO's staff members and/or volunteers collect, disclose, access, maintain, store, or use any of their PII, for CDO and CDO's staff members and volunteers to: create, collect, disclose, access, maintain, store, and use their PII to carry out the Authorized Functions listed at Section III.2 of this Agreement. This authorization may be obtained either directly from the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and/or Qualified Employer, or through such person(s)' representative(s) or Authorized Representative(s). CDO and its staff members and/or volunteers may use the model form provided by CMS and appended hereto and referred to as Appendix E to fulfill this requirement. This authorization is separate and distinct both from any authorization obtained pursuant to section III.7 of this agreement and from the informed consent referenced in Appendix A

at 3(a). CDO must ensure that it or its staff members and/or volunteers maintain a record of it; and

c. May revoke at any time the authorization provided pursuant to 155.225(f).

9. Oversee and monitor any staff member or volunteer it certifies as a CAC to ensure that each CAC complies with all requirements of the program specified in 45 CFR 155.225, and with all requirements set forth in Section II.2 of this Agreement.

10. Establish and comply with procedures to do the following:

    a. As soon as possible, but in no event later than 20 Days after the triggering event (identification or notification of noncompliance), withdraw the certification of any staff member or volunteer that has been certified by the CDO if the CDO learns or is notified by CMS that the staff member or volunteer has failed to comply with the terms and conditions of the CAC's agreement with the CDO or with the requirements of 45 CFR 155.225;

    b. Protect any PII of Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) created, collected, disclosed, accessed, maintained, stored, or used by any CAC whose certification is withdrawn, by complying with the obligations set forth in Section VI of this Agreement;

    c. As soon as possible, but in no event later than 20 Days after the CDO learns that any staff members or volunteers who have been certified as CACs are out of compliance with the terms and conditions of the agreement required by Section II.2.b of this Agreement, or with any of the requirements of 45 CFR 155.225, or upon notification from CMS that the CDO must withdraw certification from any specific staff member and/or volunteer, notify the certified staff member or volunteer that he or she must, immediately upon receipt of this notice, cease holding out him- or herself as a CAC to any Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and/or Qualified Employer, and/or these individuals' legal representative(s) or Authorized Representative(s), and cease providing CAC services to the public;

    d. As soon as possible, but in no event later than 20 Days after notification from CMS that the CDO's designation as a CDO has been withdrawn, ensure that all staff members and volunteers refrain from holding themselves out as CACs and refrain from providing CAC services to the public.

11. Not impose any charge on Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s) for application or other assistance related to the Exchange; and

12. Comply with the privacy and security standards adopted by the FFE pursuant to 45 C.F.R. § 155.260(b), and applicable authentication and data security standards, in the manner set forth in section III and Appendix A of this Agreement;

13. Directly, or through its staff or volunteers it certifies as CACs, provide any and all services in connection with the obligations and conditions in this Agreement, as described in Section II.1-13 and III of this Agreement, without compensation (excluding wages earned by employees of the CDO for work performed by such employee on behalf of its CDO employer), and hereby waive its rights to any compensation from the Government of the United States of America to which it may be entitled under law.

III. OBLIGATIONS RELATED TO THE PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION.

1. CDO hereby acknowledges and agrees to accept and abide by the standards and implementation specifications set forth below and in Appendix A, "Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities," which is incorporated by reference in this Agreement, when engaging in any activity as a CDO pursuant to 45 CFR 155.225. CDO is thereby bound to strictly adhere to the privacy and security standards, and to ensure that its Workforce that creates, collects, accesses, stores, maintains, discloses, or uses PII, is contractually bound to strictly adhere to the equivalent standards and implementation specifications, so as to ensure the efficient operation of the FFE.

2. Authorized Functions. CDO may create, collect, disclose, access, maintain, store, and use PII of Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representative(s) or Authorized Representative(s) in order to:

    a. Provide information to these persons about the full range of QHP options and Insurance Affordability Programs for which these persons are eligible;

    b. Assist these persons with applications for coverage in a QHP through the FFE and for Insurance Affordability Programs;

    c. Help to facilitate the enrollment of these persons in QHPs and Insurance Affordability Programs; and

    d. Perform other functions authorized under 45 CFR 155.225, including functions substantially similar to those enumerated above, and such other functions that may be approved by CMS in writing from time to time.

3. PII Received. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, CDO, may create, collect,

disclose, access, maintain, store, and use the following data and PII from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s):

APTC percentage and amount applied
Auto disenrollment information
Applicant Name
Applicant Address
Applicant Birthdate
Applicant Telephone number
Applicant Email
Applicant spoken and written language preference
Applicant Medicaid Eligibility indicator, start and end dates
Applicant Children's Health Insurance Program eligibility indicator, start and end dates
Applicant QHP eligibility indicator, start and end dates
Applicant APTC percentage and amount applied eligibility indicator, start and end dates
Applicant household income
Applicant Maximum APTC amount
Applicant Cost-sharing Reduction (CSR) eligibility indicator, start and end dates
Applicant CSR level
Applicant QHP eligibility status change
Applicant APTC eligibility status change
Applicant CSR eligibility status change
Applicant Initial or Annual Open Enrollment Indicator, start and end dates
Applicant Special Enrollment Period eligibility indicator and reason code
Contact Name
Contact Address
Contact Birthdate
Contact Telephone number
Contact Email
Contact spoken and written language preference
Enrollment group history (past six months)
Enrollment type period
FFE Applicant ID
FFE Member ID
Issuer Member ID
Net premium amount
Premium Amount, start and end dates
Pregnancy indicator
Special enrollment period reason
Subscriber Indicator and relationship to subscriber
Social Security Number
Tobacco use indicator and last date of tobacco

4. Authorization. Prior to creating, collecting, disclosing, accessing, maintaining, storing, or using any PII from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s), CDO will ensure that the CAC obtains the authorization required under Section II.8 of this Agreement to create, collect, disclose, access, maintain, use, or store their PII to carry out the Authorized Functions listed at Section III.2 of this Agreement, and will permit the authorization to be revoked at any time. CDO and its staff members and/or volunteers may use the model form provided by CMS and appended hereto and referred to as Appendix E to fulfill this requirement. This authorization is separate and distinct from any authorization obtained pursuant to section III.7 of this agreement and the informed consent referenced in Appendix A at 3(a). The CDO should ensure that a record of the authorization provided is maintained in a manner consistent with the privacy and security standards set forth in Appendix A.

5. Collection of PII. PII collected from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s), may be used only for the Authorized Functions specified in Section III.2 of this Agreement. Such information may not be reused for any other purpose.

6. Storing PII. Other than documentation related to the authorization required by Section III.4 above, CDO is not expected or required to maintain or store any of the above listed PII as a result of carrying out the Authorized Functions specified in Section III.2 above. To the extent that a CDO does maintain or store PII, such as documentation related to the authorization required by Section III.4, it must agree to comply with all provisions of this Agreement and Appendix A that apply to the maintenance or storage of PII.

7. Collection and Use of Information Provided Under Other Authorities. This Agreement does not preclude CDO from separately collecting information from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s), for a non-FFE purpose, and using, reusing, and disclosing such non-FFE information obtained separately as permitted by applicable law and/or other applicable authorities. Such information must be separately collected and stored from any PII collected in accordance with this Agreement. Any authorization for collection and use of PII under this provision is separate and distinct from the authorization obtained pursuant to Section III.4 above and II.2.b.vii and II.8, and should be obtained and maintained separately from that authorization.

8. Ability of Consumer to Limit Collection and Use. CDO agrees to allow the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and Qualified Employer, directly or through these individuals' legal representative(s) or Authorized Representative(s), to limit the CDO's creation, collection, use, maintenance, storage, and disclosure of their PII to the sole purpose of obtaining CDO's assistance for FFE purposes, and for performing Authorized Functions specified in Section III.2 of this Agreement.

IV. EFFECTIVE DATE; TERM AND RENEWAL.

a. Effective Date and Term. This Agreement becomes effective on the date the last of the two Parties executes this Agreement and ends one year from the effective date.

b. Renewal. This Agreement will automatically renew for subsequent and consecutive one (1) year periods upon the expiration of this agreement unless, in the sole and absolute discretion of CMS, thirty (30) Days' advance written notice of nonrenewal is provided by CMS to CDO, or the Agreement is terminated pursuant to Section V of this Agreement.

V. TERMINATION.

a. Termination without Cause. Either Party may terminate this Agreement without cause and for its convenience upon at least thirty (30) Days' prior written notice to the other Party. Such notice will include the effective date on which the organization will no longer have its staff members or volunteers provide CAC services. This Agreement shall automatically terminate at the end of its term or in connection with the rejection of an amendment as provided for in Section VII.h of this Agreement.

b. Termination with Cause. CMS may terminate this Agreement for cause, as follows:

i. Termination with Notice. This Agreement shall terminate immediately upon CMS's withdrawal of CDO's designation as a CDO. CMS may terminate this Agreement upon fourteen (14)-Days' written notice to CDO if CDO materially breaches any term of this Agreement as determined at the sole but reasonable discretion of CMS, unless CDO commences curing such breach(es) within such 14-Day period to the reasonable satisfaction of CMS, and thereafter diligently prosecutes such cure to completion. The 14-Day notice from CMS shall contain a description of the material breach, whereupon CDO 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, which plan and time frame may be rejected, approved or amended in CMS's sole but reasonable discretion. Notwithstanding the foregoing, CDO shall be considered in "Habitual Default" of this Agreement in the event that it has been served with a 14-Day notice under this subsection more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately thereafter terminate this Agreement upon notice to CDO without any further opportunity to cure or propose cure.

c. Consequences of Termination or Nonrenewal. If this Agreement is not renewed pursuant to Section IV.b or is terminated pursuant to Sections V.a or V.b of this Agreement, CDO's designation is automatically withdrawn. If that occurs CDO must immediately cease holding out as a CDO to any Consumer, Applicant,

Qualified Individual, Enrollee, Qualified Employee, and Qualified Employer, and/or these individuals' legal representative(s) or Authorized Representative(s), must immediately cease providing CAC services to the public through its staff members and volunteers, and must carry out procedures described in II.10.

VI. DESTRUCTION OF PII. CDO covenants and agrees to destroy all PII in its possession at the end of the record retention period required under Appendix A. If, upon the termination or expiration of this Agreement, CDO has in its possession PII for which no retention period is specified in Appendix A, such PII shall be destroyed within 30 Days of the termination or expiration of this Agreement. CDO's duty to protect and maintain the privacy and security of PII, as provided for in Appendix A of this Agreement, shall continue in full force and effect until such PII is destroyed and shall survive the termination or expiration of this Agreement.

VII. MISCELLANEOUS

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

If to CMS:
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 CDO, to CDO'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 facsimile 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. CMS and CDO may change their contact information for notices and other communications by providing thirty (30) Days' written notice of such change in accordance with this provision.

b. Assignment and Subcontracting. CDO shall not assign this Agreement in whole or in part, whether by merger, acquisition, consolidation, reorganization or otherwise, nor subcontract any portion of the services to be provided by CDO under this Agreement, nor otherwise delegate any of its obligations under this Agreement, without the express, prior written consent of CMS, which consent may be withheld, conditioned, granted or denied in CMS's sole and absolute discretion. CDO further shall not assign this Agreement or any of its rights or

obligations hereunder without the prior written consent of the State. If CDO attempts to make an assignment, subcontract its service obligations or otherwise delegate its obligations hereunder in violation of this provision, such assignment, subcontract or delegation shall be deemed void *ab initio* and of no force or effect, and CDO shall remain legally bound hereto and responsible for all obligations under this Agreement. CDO shall further be thereafter subject to such compliance actions as may otherwise be provided for under applicable law.

c. 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.

d. Disclaimer of Joint Venture. Neither this Agreement nor the activities of CDO 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 CDO. Neither CMS or CDO is, nor shall either CMS or CDO hold itself out to be, vested with any power or right to bind the other contractually or to act on behalf of the other, except to the extent expressly set forth in ACA and the regulations codified thereunder, including as codified at 45 CFR part 155.

e. 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.

f. Compliance with Law. CDO 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 which constitutes the stricter, higher or more stringent level of compliance shall control.

g. Governing Law. This Agreement shall be governed by the laws and common law of the United States of America, including without limitation such regulations as may be promulgated from time to time by the HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. CDO 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*.

h. Amendment. CMS may amend this Agreement for purposes of reflecting changes in applicable law, regulations, or CMS implementation guidance, with such amendments taking effect upon thirty (30) Days' written notice to CDO ("CMS notice period"). Any amendments made under this provision will only have prospective effect and will not be applied retrospectively. CDO may reject such amendment, by providing to CMS, during the CMS notice period, thirty (30) Days' 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.

i. Audit. CDO agrees that CMS, the Office of the Inspector General of HHS, and the Comptroller General, as applicable, or their designees have the right to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of CDO compliance with the requirements of this Agreement, upon reasonable notice to CDO and during CDO's regular business hours and at CDO's regular business location. CDO further agrees to allow reasonable access to the information and facilities requested by CMS, the Office of the Inspector General of HHS, and the Comptroller General, as applicable, or their designees for the purpose of such an audit.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

This Agreement between CDO and the Centers for Medicare & Medicaid Services for the Federally-facilitated Exchange has been signed by:

FOR CDO

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

Signature of Senior Official of **CDO**

Name and Title of Senior Official of **CDO**

Date

CDO Name

CDO Designated ID Number

CDO Address

FOR CMS

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

_____ _____

Kevin J. Counihan **Date**
Director
Center for Consumer Information & Insurance Oversight
Centers for Medicare & Medicaid Services

_____ _____

Todd Lawson **Date**
Acting Director
Office of E-Health Standards and Services
Centers for Medicare & Medicaid Services

APPENDIX A

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 Affordable Care Act (42 U.S.C. § 18081(g)) and 45 CFR 155.260. As used in this document, all terms used herein carry the meanings assigned in Appendix B, attached to this Agreement.

The standards and implementation specifications that are set forth in this Appendix A and Version 1.0 of the Minimum Acceptable Risk Standards—Exchanges (MARS-E) suite of documents (which can be found at http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/) are the same as, or more stringent than, the privacy and security standards and implementation specifications that the Centers for Medicare and Medicaid Services ("CMS") has established for the Federally-Facilitated Exchanges ("FFEs") established under Section 1321(c) of the Affordable Care Act (42 U.S.C. § 18041(c)).

CMS will enter into contractual agreements with Non-Exchange Entities that gain access to Personally Identifiable Information ("PII") exchanged with the FFEs, or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s). Each such agreement and its appendices, which include this Appendix A, govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by the Non-Exchange Entity in the context of the FFE. In signing any such contractual agreement, in which this Appendix A has been incorporated, a Non-Exchange Entity agrees to comply with the standards and implementation specifications laid out in this document and the referenced MARS-E suite of documents while performing the Authorized Functions outlined in the agreement.

NON-EXCHANGE ENTITY PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS

In addition to the standards and implementation specifications set forth in the MARS-E suite of documents noted above, Non-Exchange Entities must meet the following privacy and security standards and implementation specifications to the extent they are not inconsistent with any applicable MARS-E standards.

(1) *Individual Access to PII: In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities that maintain and/or store PII must provide Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) and Authorized Representative(s), 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: 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 the FFE.
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, Enrollees, Qualified Employees, and Qualified Employers 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, Qualified Employees, Qualified Employers and/or these individuals' legal representative(s) or Authorized Representative(s) 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. Unless the Non-Exchange Entity is a Certified Application Counselor Designated Organization or Certified Application Counselor, it may charge a fee only to recoup its costs for labor for copying the PII, supplies for creating a paper copy or a copy on electronic media, postage if the PII is mailed, or any costs for preparing an explanation or summary of the PII if the recipients 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. Under no circumstances may Certified Application Counselor Designated Organizations or Certified Application Counselors charge any consumers any fees for application or other assistance related to the Exchange
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 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. Unreviewable grounds for denial. 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;
    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 FFE, Non-Exchange Entities must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees, and/or these individuals' legal representative(s) or Authorized Representative(s), 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 Web site, 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 accessible and timely 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;
    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 Web site, 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 Web site.

(3) *Individual choice. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities should ensure that Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representative(s) or Authorized Representative(s), 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, Enrollees, Qualified Employees, Qualified Employers or these individuals' legal representative(s) or Authorized Representative(s), only for the functions and purposes listed in the Privacy Notice Statement and any relevant agreements in effect as of the time the information is collected, unless the FFE 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);
    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 10 years.

(4) *Creation, collection, disclosure, access, maintenance, storage, and use limitations. In keeping with the standards and implementation specifications used by the FFE, 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, Enrollee, Qualified Employee, Qualified Employer, and/or these individuals' legal representative(s) or Authorized Representative(s).*

a. Standard: 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:

1. To the extent necessary to ensure the efficient operation of the Exchange;

2. 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
3. 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, Enrollee, Qualified Employee, or Qualified Employer when the information may 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 employing marketing practices or benefit designs that will have the effect of discouraging the enrollment of individuals with significant health needs in Qualified Health Plans ("QHPs").

(5) *Data quality and integrity. In keeping with the standards and implementation specifications used by the FFE, 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 FFE, Non-Exchange Entities must offer Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal

representative(s) or Authorized Representative(s), 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 Information 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 telephonically. They may also be offered an opportunity to meet with such individual 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;
    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 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 FFE, 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 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 amendment, correction, substitution, or deletion of a Consumer's, Applicant's, Qualified Individuals', Enrollee's, Qualified Employee's, or Qualified Employer'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, school identification card, 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 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, Enrollees, Qualified Employees, Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s), 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 FEE, Non-Exchange Entities should adopt and implement the standards and implementation specifications in this document and the cited MARS-E document suite, 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 Procedures[1] and memorialized in the Non-Exchange Entity's own written policies and procedures. Such policies and procedures would:
   i. Identify the Non-Exchange Entity's Designated Privacy Official, if applicable, and/or identify other personnel authorized to access PII and responsible for reporting and managing Incidents or Breaches to CMS.
   ii. 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
   iii. Require reporting any 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 required time frames.

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

[1] Available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_7-1_Incident_Handling_Standard.pdf

disclosure; and/or the submission of a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures.

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

a. Standard: Training and Awareness. The Non-Exchange Entity shall develop training and awareness programs for members of its Workforce that create, collect, disclose, access, maintain, store, and use PII while carrying out any Authorized Functions.

   i. Implementation Specifications:

      1. The Non-Exchange Entity must require such individuals to successfully complete privacy and security training, as appropriate for their work duties and level of exposure to PII, prior to when they assume responsibility for/have access to PII.
      2. The Non-Exchange Entity must require periodic role-based training on an annual basis, at a minimum.
      3. The successful completion by such individuals of applicable training programs, curricula, and examinations offered through the FFE is sufficient to satisfy the requirements of this paragraph.

b. Standard: Security Controls. The FFE shall adopt and implement the Security Control standards cited in the MARS-E document suite for protecting the confidentiality, integrity, and availability of PII.

   i. Implementation Specifications:

      1. Implementation specifications for each Security Control are provided in the MARS-E document suite.

APPENDIX B

DEFINITIONS

This Appendix defines terms that are used in the Agreement and other Appendices. Any capitalized term used in the Agreement that is not defined here has the meaning provided in 45 CFR 155.20.

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

(2) **Access** means availability of a SORN Record to a subject individual.

(3) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 CFR 155.20.

(4) **Applicant** has the meaning set forth in 45 CFR 155.20.

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

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

(7) **Breach** is defined by OMB Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information (May `22, 2007), as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control or any similar term or phrase that refers to situations where persons other than authorized users or for an other than authorized purpose have access or potential access to Personally Identifiable Information (PII), whether physical or electronic.

(8) **CAC Certificate** means the certificate issued to each CAC by his or her CDO, indicating that he or she has been certified as a CAC, and containing the CAC's name and unique CAC identification number.

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

(10) **Certified Application Counselor** (CAC) means a staff member or volunteer who is certified by a Certified Application Counselor Designated Organization to perform the duties and meet the standards and requirements for CACs in 45 CFR 155.225.

(11) **Certified Application Counselor Designated Organization** (CDO) means an organization designated by the Federally-facilitated Exchange to certify its staff members or volunteers to act as CACs.

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

(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) **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 other Insurance Affordability Program, or whom an agent or broker (including Web-brokers), Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a coverage through QHP, applying for Advance Payments of the Premium Tax Credits (APTCs) and Cost-sharing Reductions (CSRs), and/or completing enrollment in a QHP through its web site for individual market coverage.

(15) **Cost-sharing Reduction (CSR)** has the meaning set forth in 45 CFR 155.20.

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

(17) **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 notice, responsible for the development and implementation of the privacy and security policies and procedures of the Non-Exchange Entity, and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy and security of PII.

(18) **Enrollee** has the meaning set forth in 45 CFR 155.20.

(19) **Exchange** has the meaning set forth in 45 CFR 155.20.

(20) **Federally-facilitated Exchange (FFE)** means an **Exchange** (or **Marketplace**) established by HHS and operated by CMS under Section 1321(c)(1) of the ACA for individual or small group market coverage, including the Federally-facilitated Small Business Health Options Program (**FF-SHOP**). **Federally-facilitated Marketplace (FFM)** has the same meaning as FFE.

(21) **HHS** means the U.S. Department of Health & Human Services.

(22) **Incident**, or **Security Incident**, means the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

(23) **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.

(24) **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 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 Affordable Care Act.

(25) **Minimum Acceptable Risk Standards—Exchanges (MARS-E)** means a CMS-published suite of documents, version 1.0 (August 1, 2012), that defines the security standards required pursuant to 45 CFR 155.260 and 45 CFR 155.270, for any Exchange, individual, or entity gaining access to information submitted to an Exchange or through an Exchange using a direct, system-to-system connection to the Hub, available on the CCIIO web site.

(26) **Navigator** has the meaning set forth in 45 CFR 155.20.

(27) **Non-Exchange Entity** has the meaning at 45 CFR 155.260(b), including but not limited to Navigators, agents, and brokers.

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

(29) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-07-16 (May 22, 2007) and means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, *etc.*, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

(30) **Qualified Employee** has the meaning set forth in 45 CFR 155.20.

(31) **Qualified Employer** has the meaning set forth in 45 CFR 155.20.

(32) **Qualified Health Plan (QHP)** has the meaning set forth in 45 CFR 155.20.

(33) **Qualified Individual** has the meaning set forth in 45 CFR 155.20.

(34) **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.

(35) **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.

(36) **State** means the State where the Certified Application Counselor that is a party to this Agreement is operating.

(37) **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.

(38) **Subject Individual** means that individual to whom a SORN Record pertains.

(39) **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.

(40) **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.

(41) **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.

(42) **Training Certificate** means the certificate issued to each potential CAC by the Medicare Learning Network upon their completion of the required CMS-approved training courses and examinations.

(43) **Web** means the World Wide Web.

(44) **Workforce** means a Non-Exchange Entity's or FFE'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 E

Model Certified Application Counselor (CAC) Authorization Form

In Federally-Facilitated or State Partnership Marketplaces

CAC Designated Organization Name and Address:

_____

CAC Designated Organization Phone Number and Email:

_____

Individual CAC Name and Certification Number:

_____

I, _____, give my permission, or _____ [Insert name of authorized representative], my legal or Marketplace authorized representative acting on my behalf ("authorized representative"), gives permission to _____ _____[Names][1] to create, collect, disclose, access, maintain, use, and/or store my personally identifiable information (PII) and/or the PII of my authorized representative, to perform the following duties of a CAC Designated Organization or CAC[2]:

- Inform me and/or my authorized representative about the full range of Marketplace health coverage options and insurance affordability programs for which I'm eligible;
- Help me complete my application for health coverage in a Qualified Health Plan (QHP) through the Marketplace and for insurance affordability programs;
- Help me enroll in a QHP or in an insurance affordability program.

I understand that I may revoke this authorization at any time and will notify _____ _____ [Names] if I choose to revoke my authorization.

I understand that _____ _____ [Names] have the following responsibilities and will perform the following functions:

- _____ [Names] will inform me and/or my authorized representative about the full range of Marketplace health coverage options and insurance affordability programs for which I'm eligible, will help me apply for health coverage in a QHP through the Marketplace and for insurance affordability programs, and will help me enroll in a QHP or in an insurance affordability program.
- _____ [Names] will inform me of any possible conflicts of interest they might have.
- _____ [Names] can't choose a health insurance plan for me.

---

[1] NOTE TO CAC DESIGNATED ORGANIZATION AND INDIVIDUAL CAC: Each time [Names] appears in this Authorization Form, the Name of the CAC Designated Organization *and* the name of the individual staff/volunteer CAC should be inserted on the blank line in front of [Names].

[2] These duties are set forth in 45 CFR §155.225.

- _____ [Names] is required to act in my best interest.

- _____ [Names] will follow privacy and information security standards when creating, collecting, disclosing, accessing, maintaining, storing, and/or using my PII and/or the PII of my authorized representative. Information about these standards will be provided.
- _____ [Names] aren't expected or required to maintain or store any of my PII and/or the PII of my authorized representative, other than this authorization form, but if _____ _____ [Names] do maintain or store my PII, they will follow privacy and information security standards.
- I and/or my authorized representative do not need to provide _____ _____ [Names] contact information, unless I want _____ [Names] to follow-up with me on applying for or enrolling into coverage. My consent to follow-up is given by providing my phone number and/or e-mail address below.
- _____ [Names]
- I and/or my authorized representative don't have to give _____ _____ [Names] more information than I and/or my authorized representative choose to provide.
- The assistance _____ [Names] provide is based only on the information I and/or my authorized representative provide, and if the information provided is inaccurate or incomplete, _____ _____ [Names] may not be able to provide all the assistance available for my situation.
- If _____ [Names] are unable to assist me and/or my authorized representative, they will refer me or my authorized representative to another person who can help me (a Navigator or other Marketplace-authorized assistance personnel), or to the Exchange call center.
- _____ [Names] won't charge me and/or my authorized representative a fee for any assistance provided.

Please sign and date the form:

_____

Signature of Consumer/Consumer's Legal or Marketplace Authorized Representative (please circle a status to indicate whether you're the consumer or the consumer's representative)

Date _____

_____

Phone Number and E-Mail Address for Follow-Up (Optional)

PLEASE NOTE: Consumers may sign this authorization form themselves, or choose to have a legal or Marketplace Authorized Representative complete this form.

APENDICE E

Formulario de Autorización Para Consejero Certificado para Solicitantes

En Mercados de Seguros Médicos Facilitados por el Estado o en Mercados Estatales

Nombre y Dirección del Consejero Certificado Determinado:

_____

Número de Teléfono y Dirección de Correo Electrónico del Consejero Certificado Determinado:

_____

Nombre y Número de Certificación del Consejero Certificado:

_____

Yo, _____, otorgo mi permiso, o delego a _____ [Añadir el nombre del representante autorizado], mi representante legal o represéntate autorizado en el mercado de seguros médicos ("representante autorizado"), otorgo permiso para _____ _____[Nombres][1] para crear, recoger, publicar, acceder, mantener, usar, y/o guardar mi información personal identificable) y/o la información personal identificable de mi representante autorizado, para desempeñar las siguientes funciones como consejero certificado[2]:

- Informarme o a mi representante autorizado acerca de todas las opciones de cobertura medica y programas de seguros asequibles en el mercado de seguros que yo sea elegible;
- Ayudarme a completar los formularios para cobertura de salud en un plan calificado a través del Mercado de seguros o en un programa de seguro asequible;
- Ayudarme a inscribirme en un plan calificado de salud o en un programa de seguro asequible.

Yo entiendo que puedo revocar esta autorización en cual momento y notificare _____ _____ [Nombre] si es que decido revocar mi autorización.

- Yo entiendo que_____ _____ [Nombre] tienen las siguientes responsabilidades y desempeñaran las siguientes funciones: _____ [Nombres] Informarme y/o a mi representante autorizado acerca de todas las opciones de cobertura medicas y programas de seguros asequibles en el mercado de seguros que yo sea elegible;
- Ayudarme a completar los formularos para cobertura de salud en un plan calificado a través del Mercado de seguros o en un programa de seguro asequible;
- Ayudarme a inscribirme en un plan calificado de salud o en un programa de seguro asequible.

---

[1] Nota Para Consejeros Certificado para Solicitantes (Organización/Individual): Cada vez [Nombres] aparecen en este formulario de autorización, el nombre del consejero certificado debe ser añadido a la línea en blanco en frente a [Nombres].

[2] Estas responsabilidades están requeridas en 45 CFR §155.225.

- _____ [Nombres] me informara de cualquier posible conflicto de interés que puedan tener
- _____ [Nombres] no puede(n) elegir un plan de seguros para me
- _____ [Nombres] esta requerido a actuar para mi beneficio

- _____ [Nombres] seguirá reglas de privacidad y seguridad para crear, recoger, publicar, acceder, mantener, usar, y/o guardar mi información personal identificable) y/o la información personal identificable de mi representante autorizado. Información acerca de estas reglas de privacidad y seguridad serán proveídas.
- _____ [Nombres] No esta supuesto o requerido a guardar mi información personal identificable) y/o la información personal identificable de mi representante autorizado, en otro formulario si no que en este formulario de autorización, pero si _____ _____ [Nombres] este si llega a mantener, usar, y/o guardar mi información personal identificable, ellos seguirán seguirá estrictas reglas de privacidad y seguridad.
- Yo y/o mi representante autorizado no tenemos que proveer _____ _____ [Nombres] información para contactarme, a no ser que yo quiera _____ [Nombres] para hacer seguimiento con el propósito de aplicar o inscribirme en la cobertura de seguros médicos. Mi consentimiento para hacer este seguimiento es otorgado por medio de proveer mi número de teléfono y/o dirección de correo electrónico.
- _____ [Nombres]
- Yo y/o mi representante autorizado no tenemos que proveer_____ [Nombres] mas información, a no ser que yo quiera
- La asistencia _____ [Nombres] proveída es basado solo en la información que yo y/o mi representante autorizado proveamos, y si esta información es incorrecta o incompleta, _____ _____ [Nombres] no podrá proveer toda la asistencia disponible en mi situación.
- Si _____ [Nombre] no pueden asistirme o a mi representante autorizado, seré referido o mi representante autorizado a otra persona que pueda ayudarme (a un navegador u otra persona autorizada para asistir en el mercado de seguros médicos), o al centro de llamados.
- _____ [Names] no habrá cobro para mi o a mi representante autorizado por honorarios por cualquier asistencia proveída.

Por favor firmar e incluir la fecha en este formulario:

_____

Firma del Consumidor/ Representante Legal o represéntate autorizado en el mercado de seguros (por favor indicar con un circulo si usted es el consumidor o un representante)

Fecha _____

_____

Número de Teléfono y Dirección de Correo Electrónico Para Seguimiento (Opcional)

POR FAVOR NOTE: Consumidores pueden firmar este formulario por si mismos, o tienen la opción de elegir un representante legal o un representante autorizado en el mercado de seguros para completar este formulario.