Expiration Date: XX/XXXX

MODEL AGREEMENT BETWEEN CERTIFIED APPLICATION COUNSELOR DESIGNATED ORGANIZATION IN A STATE IN WHICH THE FEDERALLY-FACILITATED EXCHANGE IS OPERATING AND CERTIFIED APPLICATION COUNSELOR

THIS AGREEMENT ("Agreement") is entered into between _____, an organization that The Centers for Medicare & Medicaid Services ("CMS"), which manages and oversees the Federally-facilitated Exchanges ("FFEs"), has designated as a Certified Application Counselor Designated Organization in _____ [Insert name(s) of applicable FFE state(s) in which organization is designated], a State/States in which an FFE is operating (hereinafter referred to as "CDO") and _____, a staff member or volunteer of the CDO who wishes to be certified by the CDO to act as a Certified Application Counselor (hereinafter referred to as "Staff Member/Volunteer") and to perform the duties and meet the standards and requirements of 45 CFR 155.225. The CDO and Staff Member or Volunteer are hereinafter sometimes referred to as "Party," or, collectively, as the "Parties."

WHEREAS:

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

2. CMS has designated CDO to certify staff members and volunteers to act as certified application counselors in an FFE.

3. Pursuant to 45 CFR 155.225(c), CACs are expected to provide the following services to Consumers:
    a. Provide information about the full range of Qualified Health Plan (QHP) options and Insurance Affordability Programs for which Consumers are eligible which includes: providing fair, impartial, and accurate information that assists Consumers with submitting the eligibility application; clarifying the distinctions among health coverage options, including QHPs; and helping Consumers make informed decisions during the health coverage selection process;
    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.

4. The CDO, and the staff members and volunteers that the CDO certifies as CACs, will need to create, collect, disclose, access, maintain, store, and/or use the Personally Identifiable Information ("PII") from CMS and Consumers, 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. 45 CFR 155.225(d)(3) requires all CACs to comply with the Exchange's privacy and security standards adopted consistent with 45 CFR 155.260, and applicable authentication and data security standards.

6. CMS, in the administration of the FFEs, has adopted privacy and security standards for CDO, as set forth in Appendix A, "Privacy and Security Standards and Implementation Specifications for Certified Application Counselors and Certified Application Counselor Designated Organizations." Compliance with this Agreement satisfies the requirement under 45 CFR 155.225(d)(3) to comply with Exchange privacy and security standards, and 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

a. Staff Member/Volunteer's Obligations and Conditions. To carry out the functions of a CAC, as authorized by 45 CFR 155.225, and as a condition of Staff Member/Volunteer's certification by CDO, Staff Member/Volunteer agrees to the following:

i. Prior to functioning as a CAC, Staff Member/Volunteer shall seek certification by doing all of the following:

1. Register with CDO and receive a unique identifying number and a CAC Certificate, in accordance with CDO's procedures;

2. Register for all required CMS-approved training using Staff Member/Volunteer's unique CAC identification number and the name that will appear on both his or her CAC Certificate and Training Certificate;

3. Complete all required 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;

4. Complete and achieve a passing score on all CMS-approved certification examinations;

5. Provide proof in the form of his or her printed Training Certificate to CDO that he or she has fulfilled the training and certification examination requirements specified in Section II.a.i.2 through 4;

6. Meet any licensing, certification, or other standards prescribed by the State or FFE, if applicable, so long as such standards do not prevent the application of the provisions of title I of the Affordable Care Act;

7. Execute this Agreement.

ii. Staff Member/Volunteer shall disclose to CDO any relationship Staff Member/Volunteer has with QHPs or Insurance Affordability Programs, or other potential conflicts of interest;

iii. Staff Member/Volunteer shall comply with FFE's Privacy and Security Standards and Implementation Specifications for Certified Application Counselors specified in Section III and Appendix A of this Agreement

iv. When assisting Consumers, Staff Member/ Volunteer shall:

1. Follow CDO's established procedures to prominently display to Consumers a current and effective CAC Certificate provided by CDO evidencing the individual's certification as a CAC each time Staff Member/Volunteer assists any Consumers;

2. Follow CDO's established procedures to inform Consumers of the functions and responsibilities of CACs;

3. Follow CDO's established procedures to obtain the authorization required by 45 CFR 155.225(f) and section III.d of this Agreement, prior to creating, collecting, disclosing, accessing, maintaining, storing, or using any PII of Consumers to carry out the Authorized Functions listed at Section III.b of this Agreement. This authorization is separate and distinct from any informed consent obtained pursuant to section 2(b) of Appendix A of this Agreement;

4. Follow CDO's established procedures to maintain a record of the authorization provided under Section III.d for a period of no less than

six (6) years, unless a different and longer retention period has already been provided under other applicable Federal law;

5. Permit the Consumer to revoke the authorization described in Section III.d at any time;

6. Provide his or her unique CAC identification number to any Consumer being assisted so that the application reflects that he or she has provided assistance;

7. Not impose any charge or fee on Consumers for application or other assistance related to the FFE;

8. Act in their best interest;

9. 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 FFE call center, 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;

10. Provide information to them about the full range of QHP options and Insurance Affordability Programs for which they are eligible, which includes: providing fair, impartial, and accurate information that assists Consumers with submitting the eligibility application; clarifying the distinctions among health coverage options, including QHPs; and helping Consumers make informed decisions during the health coverage selection process;

11. Assist them in applying for coverage in a QHP through the FFE and for Insurance Affordability Programs;

12. Help to facilitate their enrollment in QHPs and Insurance Affordability Programs;

13. Follow CDO's procedures to disclose to them any relationships the CAC has with QHPs or Insurance Affordability Programs, or other potential conflicts of interest;

14. [FOR USE ONLY IF THE CDO DECIDES TO REQUIRE THIS] Follow CDO's procedures to disclose to them any relationship the CDO has with QHPs or Insurance Affordability Programs, or other potential conflicts of interest, using language supplied by CDO;

15. Not provide gifts, including gift cards or cash, unless they are of Nominal Value, or provide promotional items that market or promote the products or services of a third party, to any Applicant or potential Enrollee as an inducement for enrollment. Gifts, gift cards, or cash may exceed Nominal Value for the purpose of providing reimbursement for legitimate expenses incurred by a Consumer in an effort to receive Exchange application assistance, such as, but not limited to, travel or postage expenses;

16. Not solicit any Consumer for application or enrollment assistance by going door-to-door or through other unsolicited means of direct contact, including calling a Consumer to provide application or enrollment assistance without the Consumer initiating the contact, unless the individual has a pre-existing relationship with the individual CAC or the CDO, and other applicable State and Federal laws are otherwise complied with. Outreach and education activities may be conducted by going door-to-door or through other unsolicited means of direct contact, including calling a Consumer; and

17. Not initiate any telephone call to a Consumer using an automatic telephone dialing system or an artificial or prerecorded voice, except in cases where the individual certified application counselor or designated organization has a relationship with the Consumer and so long as other applicable State and Federal laws are otherwise complied with.

v. For as long as the CAC continues providing CAC services, seek recertification on at least an annual basis after successfully completing recertification training;

vi. 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, and immediately cease providing CAC services to the public;

vii. Not sell or otherwise transfer information that was provided to the CAC by Consumers to any person or entity other than for such actions as are specifically permitted by this Agreement or as expressly authorized;

viii. Not collect or otherwise maintain information provided by Consumers, except as specifically provided for in this Agreement;

ix. Not receive any consideration directly or indirectly from any health insurance issuer or issuer of stop-loss insurance in connection with the enrollment of any individuals in a QHP or non-QHP. This prohibition does not apply to consideration the CAC receives from a health insurance issuer for health care services provided; and

x. As evidenced by my signature hereon, I hereby agree to provide the duties and services described herein without compensation of any kind (other than the wages I may nonetheless earn as an employee of CDO for work performed on behalf of my employer), and hereby waive my rights to any fee, remuneration or compensation to which I might somehow be entitled to receive from the Government of the United States of America under applicable law.

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

a. Staff Member/Volunteer 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 Certified Application Counselors and Certified Application Counselor Designated Organizations," which is incorporated by reference in this Agreement, when engaging in any CAC Authorized Function pursuant to 45 CFR 155.225. Staff Member/ Volunteer is thereby bound to strictly adhere to the privacy and security standards.

b. Authorized Functions. Staff Member/Volunteer may create, collect, disclose, access, maintain, store, and use PII of Consumers in order to:

i. Provide information to Consumers about the full range of QHP options and Insurance Affordability Programs for which these persons are eligible, which includes: providing fair, impartial, and accurate information that assists Consumers with submitting the eligibility application; clarifying the distinctions among health coverage options, including QHPs; and helping Consumers make informed decisions during the health coverage selection process;

ii. Assist Consumers with applications for coverage in a QHP through the FFE and for Insurance Affordability Programs;

iii. Help to facilitate the enrollment of Consumers in QHPs and Insurance Affordability Programs;

iv. Perform other functions related to carrying out additional obligations as may be required under applicable state law or regulation, provided that (1) such a state requirement does not prevent the application of the provisions of title I of the Affordable Care Act within the meaning of section 1321(d) of the Affordable Care Act, and (2) Staff Member/Volunteer notifies Consumers in advance, in writing, that collection, handling, disclosure, access maintenance, storage, and/or use of their PII might be required under applicable state law or regulations. Staff Member/Volunteer should provide the required notification through the authorization obtained in accordance with 155.225(f); and

v. 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 CDO in writing from time to time, but only if CMS has expressly permitted CDO to carry out those functions.

c. PII Received. Subject to the terms and conditions of this Agreement and applicable laws, in performing the Authorized Functions under this Agreement, Staff Member/ Volunteer may create, collect, disclose, access, maintain, store, and use the following data and PII from Consumers, including but not limited to:

Access to or enrollment in employer or other health coverage
American Indian/Alaska Native status
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
Citizenship Status
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
Gender
Immigration document type and document numbers
Issuer Member ID
Membership in a Federally recognized tribe
Net premium amount
Pregnancy indicator
Premium Amount, start and end dates
Race/ethnicity
Sex
Special enrollment period reason
Subscriber Indicator and relationship to subscriber
Social Security Number
Tax filing status (tax filer, tax dependent, non-filer)
Tobacco use indicator and last date of tobacco

d. Authorization. Before Staff Member/Volunteer creates, collects, discloses, accesses, maintains, stores, or uses any of a Consumer's PII, Staff Member/Volunteer will obtain from the Consumer the authorization required by 45 CFR 155.225(f) for Staff Member/Volunteer to create, collect, disclose, access, maintain, store, and use the Consumer's PII to carry out the Authorized Functions listed at Section III.b of this Agreement, and will permit the authorization to be revoked at any time. This authorization is separate and distinct from any informed consent obtained pursuant to section 2(b) of Appendix A of this Agreement. The Staff Member/Volunteer 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.

e. Collection of PII. Except for collections, uses or disclosures that are specifically authorized by Consumers in accordance with Section 2(b) of Appendix A, PII collected from Consumers may be used only for the Authorized Functions specified in Section III.b of this Agreement.

f. Storing PII. To the extent that Staff Member/Volunteer maintains or stores PII, he or she must agree to comply with all provisions of this Agreement and Appendix A that apply to the maintenance or storage of PII.

g. Ability of Consumer to Limit Collection and Use. Staff Member/Volunteer agrees to allow the Consumer to limit Staff Member/Volunteer's creation, collection, use, maintenance, storage, and disclosure of their PII to the sole purpose of obtaining Staff Member/Volunteer's assistance for FFE purposes, and for performing Authorized Functions specified in Section III.b 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 signs 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:

i. CDO is no longer designated by CMS; or
ii. CDO, in its sole and absolute discretion, notifies Staff Member/Volunteer with thirty (30) Days' advance written notice that it has determined that the Agreement will not be renewed. Such notice will specify whether and under what conditions CDO will renew the Agreement; or
iii. CDO terminates the Agreement 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.

b. Termination with Cause. This Agreement shall terminate immediately when Staff Member/Volunteer no longer holds a position as a staff member or volunteer at CDO, or when CDO withdraws Staff Member/Volunteer's certification as a CAC, or when CMS has withdrawn CDO's designation as a CDO. CDO may terminate this Agreement for cause as soon as possible, but in no event later than twenty (20) Days

after the triggering event (identification or notification of noncompliance) if CDO learns or is notified by CMS that Staff Member/Volunteer has failed to comply with the terms and conditions of this Agreement or with any applicable requirements of 45 CFR 155.225, unless Staff Member/Volunteer commences curing such breach(es) within such 20-Day period to the reasonable satisfaction CDO, and thereafter diligently implements such cure to completion. The 20-Day notice from CDO shall contain a description of the material breach, whereupon Staff Member/Volunteer 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 CDO's sole but reasonable discretion. Notwithstanding the foregoing, Staff Member /Volunteer shall be considered in "Habitual Default" of this Agreement in the event that it has been served with a 20-Day notice under this subsection more than three (3) times in any calendar year, whereupon CDO may, in its sole discretion, immediately thereafter terminate this Agreement upon notice to Staff Member/Volunteer 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, Staff Member/Volunteer's certification as a CAC is automatically withdrawn. If that occurs Staff Member/Volunteer must immediately cease holding himself or herself out as a CAC to any Consumer, must immediately cease providing CAC services to the public, and must carry out the procedures described in Section II.vi of this Agreement.

VI. DESTRUCTION OF PII. Staff Member/Volunteer covenants and agrees to destroy all PII in his or her possession at the end of the record retention period required under Appendix A. Staff Member/Volunteer'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. GENERAL PROVISIONS.

a. Assignment and Delegation. Staff Member/Volunteer shall not assign its rights or delegate its performance under this Agreement. CDO shall not assign its rights or delegate its performance under this Agreement without the express prior written consent of CMS.

b. Disclaimer of Joint Venture. Neither this Agreement nor the activities of the Parties contemplated under this Agreement shall be deemed or construed to create in any way any partnership, joint venture or agency relationship between either or both of the Parties hereto on one hand and the United States of America (or any of its agencies or departments) on the other. Neither CDO nor Staff Member/Volunteer is, nor shall either CDO or Staff Member/Volunteer hold itself out to be, vested with any

power, authority or right to act on behalf of the United States of America in any manner as an agent or representative thereof, or to bind the United States in any manner or fashion.

c. Amendments. CDO 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 Staff Member/Volunteer ("CDO notice period"). Staff Member/Volunteer may reject such amendment, by providing to CDO, during the CDO notice period, thirty (30) Days' written notice of its intent to reject the amendment ("rejection notice period"). Any such rejection of such amendment made by CDO for purposes of reflecting changes in applicable law, regulations, or CMS implementation guidance shall result in the termination of this Agreement upon expiration of the rejection notice period.

d. Compliance with Law. CDO and Staff Member/Volunteer shall 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 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 controls.

e. [Placeholder for Governing Law provision]

f. [Placeholder for Notices provision]

g. [Placeholder for Severability provision]

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

This "Agreement between CDO and Staff Member/Volunteer has been signed by:

FOR CDO:

By: _____

[Title of person authorized to enter into agreements on behalf of organization to bind the organization]

Date: _____

FOR Staff Member/Volunteer:

By: _____

Printed Name:

_____

Date: _____

APPENDIX A

PRIVACY AND SECURITY STANDARDS FOR CERTIFIED APPLICATION COUNSELORS AND CERTIFIED APPLICATION COUNSELOR DESIGNATED ORGANIZATIONS

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 Appendix, all terms used herein carry the meanings assigned in Appendix B.

Certified Application Counselor Designated Organization ("CDO") and any Certified Application Counselor certified by CDO ("CAC") must meet the following privacy and security standards and implementation specifications in performing the duties and functions outlined under 45 CFR 155.225(c) as further detailed in the 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 ("CMS-CDO Agreement") and as further detailed in the CDO's agreement with CAC ("CDO/CAC Authorized Functions").

(1) Privacy Notice Statement. Prior to collecting PII or other information from Consumers for the purpose of fulfilling a CDO/CAC Authorized Function, CDO and/or CAC must provide Consumers with a privacy notice statement. The privacy notice statement must be in writing and must be provided on, or simultaneously with, any electronic and/or paper form the CDO and/or CAC will use to gather and/or request PII or other information from Consumers. The privacy notice statement must also be prominently and conspicuously displayed on the CDO's public facing Web site, if applicable, if the CDO and/or CAC will gather or request PII or other Consumer information through that Web site.

(a) Privacy Notice Statement Requirements.

i. The privacy notice statement must be written in plain language and, to the extent possible, provided in a manner that is accessible and timely to people living with disabilities and with limited English proficiency.

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

1. A description of the information to be collected;
2. The purpose for which the information is being collected;
3. The intended use(s) of the information;
4. To whom the information may be disclosed, for what purposes, and how a record of any disclosures may be requested from the CDO;
5. What, if any, notice or opportunities for consent will be provided regarding the collection, use or disclosure of the information;

6. How the information will be secured;
7. Whether the request to collect information is voluntary or mandatory under the applicable law;
8. Effects of non-disclosure if a Consumer chooses not to provide the requested information;
9. Any rights the person may have under state or federal laws relevant to the protection of the privacy of an individual; and
10. Information on how to file complaints with CMS and the CDO related to the CDO's and CAC's activities in relation to the information.

iii. The CDO shall maintain its privacy notice statement content by reviewing and revising it 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.

(b) Notwithstanding the general requirement above to provide a written privacy notice statement prior to collecting PII or other information from Consumers, this provision does not require CDO and/or CAC to provide a written privacy notice statement to Consumers prior to collecting a Consumer's name, physical address, e-mail address, or telephone number, so long as such information will be used solely for the purpose of making subsequent contact with the Consumer to conduct a CDO/CAC Authorized Function or sending to the consumer educational information that is directly relevant to CDO/CAC Authorized Functions. Nonetheless, with regard to such names, physical addresses, e-mail addresses, or telephone numbers, CDO and/or CAC still must comply with all privacy and security standards and requirements outlined in the CMS-CDO Agreement, the agreement between CDO and CAC, and this Appendix A.

(2) Permissible Uses and Disclosures of PII. The CDO and CAC may create, collect, disclose, access, maintain, store, and use PII from Consumers only for CDO/CAC Authorized Functions identified in Section III.2 of the CMS-CDO Agreement and Section III.b of the agreement between CDO and CAC that is in effect as of the time the information is collected, unless the CDO and/or CAC obtains informed consent as described in Section 2(b) of this Appendix A.

(a) Authorization:

i. Prior to creating, collecting, disclosing, accessing, maintaining, storing, or using any Consumer PII to perform an Authorized Function, CDO and/or CAC must obtain the authorization required by 45 CFR 155.225(f), Section II.9.b of the CMS-CDO Agreement (hereinafter referred to as "authorization"), and Section III.d of the agreement between CDO and CAC. This authorization is separate and distinct from the informed consent referenced in Section 2(b) below;

ii. CDO and/or CAC must maintain a record of the authorization provided for a period of no less than six (6) years, unless a different and longer retention period has already been provided under other applicable Federal law; and

iii. CDO and CAC must permit the Consumer to revoke the authorization at any time.

(b) Informed Consent:

i. CDO and CAC must obtain informed consent from Consumers for any creation, collection, use or disclosure of information that is not authorized under the CMS-CDO Agreement and the agreement between CDO and CAC. Such informed consent must be in writing, signed by the consenting party, and subject to a right of revocation.

ii. CDO and CAC are prohibited from denying information or assistance to persons or entities that do not wish to grant consent for any creation, collection, use or disclosure of Consumer information that is not authorized under the CMS-CDO Agreement and the agreement between CDO and CAC. iii. Informed consent must:

1. Be provided in specific terms and in plain language;
2. Identify who will obtain access to the Consumer's information under the terms of the informed consent;
3. Describe the purpose for which the informed consent is being obtained;
4. Explain what information the CDO and/or CAC will use or disclose to a specific recipient(s);
5. Provide notice of a Consumer's ability to revoke the consent at any time; and
6. Include an expiration date or event, unless effectively revoked in writing by the Consumer before that date or event.

iv. Informed consent documents must be appropriately secured and retained for no less than six (6) years, unless a different and longer retention period has already been provided under other applicable Federal law.

(3) Limitations on creation, collection, disclosure, access, maintenance, storage, and use.

(a) Permissible creation and use of PII.

Other than in accordance with the informed consent procedures outlined above, the CDO and CAC shall only create, collect, disclose, access, maintain, store, or use PII it receives in its capacity as a CDO or CAC:

i. In accordance with the privacy notice statement referenced in (1) above; and/or
ii. In accordance with the CDO/CAC Authorized Functions.

(b) Prohibited requests for, collections, or uses of PII. The CDO and CAC shall not:

i. request or require a social security number, information regarding citizenship, status as a national, or immigration status for any individual who is not seeking coverage for himself or herself on an application;
ii. request information from or concerning any individual who is not seeking coverage for himself or herself, unless the information is necessary for the eligibility determination for enrollment in a Qualified Health Plan or Insurance Affordability Programs for those seeking coverage, or is required as part of a SHOP employer application under 45 C.F.R. §155.730. Such necessary information may include information on individuals who are in an individual's tax household or who live with an individual applying for coverage, including contact information, and addresses, tax filing status, income and deductions, access to employersponsored coverage, familial or legal relationships, American Indian or
Alaska Native status, or pregnancy status; or iii. use a Consumer's or any other individual's PII to discriminate against them, such as by refusing to assist individuals who have significant or complex health care needs.

(c) Accounting for Disclosures. Except for those disclosures that are necessary to carry out CDO/CAC Authorized Functions, CDOs and CACs that maintain and/or store PII shall maintain an accounting of any and all disclosures of PII. The accounting shall:

i. 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;
ii. Be retained for at least six (6) years after the disclosure, or the life of the record, whichever is longer; and
iii. Be available to CMS, or the Consumer who is the subject of the record, upon request.

(4) Safeguarding PII.

(a) CDO and CAC must ensure that PII is protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. Specifically, CDO is required to establish and CDO/CAC are

required to implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws and ensure that:

i. PII is only used by or disclosed to those authorized to receive or view it;

ii. PII is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;

iii. PII is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and

iv. PII is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with record retention requirements under the CDO-CMS Agreement and the agreement between CDO and CAC.

(b) CDO must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls.

(c) CDO must develop and CDO/CAC must utilize secure electronic interfaces when transmitting PII electronically.

(5) Incident and Breach Reporting Requirements.

(a) Reporting. CDOs must implement and comply with Breach and Incident handling procedures that are consistent with CMS' Risk Management Handbook Standard 7.1 Incident Handling and Breach Notification[1] and memorialized in the CDO's own policies and procedures. Such policies and procedures must be in writing and:

i. Identify the CDO's Designated Privacy Official, if applicable, and/or identify other personnel authorized and responsible for reporting and managing Incidents or Breaches to CMS;

ii. Address how to identify Incidents;

iii. Determine if personally identifiable information (PII) is involved in the Incidents; iv. Require all CACs to report all potential Incidents or Breaches to CDO; v. 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 **one hour** of discovery of the Incident or Breach;

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

vi. Require the completion of the CMS Security Incident Report, a copy of which is attached hereto as Appendix C or a copy of which may be found at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMSInformation-Technology/InformationSecurity/Info-Security-Library-Items/CMS1253654.html?DLPage=2&DLSort=0&DLSortDir=ascending ;

vii. Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches; and

viii. Require the CDO Designated Privacy Official and/or other authorized personnel to be available to CMS upon request.

(b) CAC must comply with CDO's Breach and Incident handling procedures.

(c) Cooperation. CDO and CAC must cooperate with CMS in resolving any Incident or Breach, including (if requested by CMS) the return or destruction of any PII; 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.

(6) Training and Awareness Requirements. The CDO shall develop role-based training and awareness programs for members of its Workforce, and CAC shall participate in such training and awareness programs. Specifically, the CDO must require members of its Workforce to successfully complete privacy and security training that is specifically tailored and relevant to their work duties and level of exposure to PII, and prior to when they assume responsibility for/have access to PII, and CAC must successfully complete such training prior to assuming responsibility for/having access to PII.

(7) Standard Operating Procedures Requirements. The CDO shall incorporate the privacy and security standards and implementation specifications required under this Appendix A, where appropriate, in its standard operating procedures that are associated with the functions authorized under the CMS-CDO Agreement involving the creation, collection, disclosure, access, maintenance, storage, or use of PII. CAC must comply with these standard operating procedures. The CDO's standard operating procedures:

(a) Must be written in plain language and be available to all of the CDO's Workforce;

(b) Must ensure the CDO/CAC'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 CMS-CDO Agreement and/or agreement between CDO and CAC; 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; and

(c) Must be designed and implemented to ensure the CDO 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 CDO, to ensure such compliance.

(8) Required Monitoring of Security Controls. CDO must monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls.

(9) Required Flow-Down of Privacy and Security Agreements. CDO must bind in a signed writing any CACs and Downstream Entities to the same privacy and security standards and obligations contained in this Appendix A.

(10) Compliance with the Internal Revenue Code. If any 'return information,' as defined in section 6103(b)(2) of the Internal Revenue Code (the Code), is accessed or used by CDO or CAC, it must be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code.

(11) Penalties for improper use and disclosure of information. CDO and CAC acknowledge that any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the Affordable Care Act will be subject to a civil money penalty, consistent with the bases and process for imposing civil penalties specified at 45 C.F.R. 155.206 and/or 155.285, in addition to other penalties that may be prescribed by law.

APPENDIX B

DEFINITIONS

This Appendix defines terms that are used in the Agreement and other Appendices to the Agreement. Any capitalized term used in the Agreement that is not defined here, or in the Agreement or other Appendices, 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) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 CFR 155.20.

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

(4) **Authorized Function** means a task performed by a Non-Exchange Entity that the NonExchange 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.

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

(6) **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 other than an authorized purpose have access or potential access to Personally Identifiable Information (PII), whether physical or electronic.

(7) **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.

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

(9) **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.

(10) **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.

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

(12) **Consumer** means an Applicant, Enrollee, Qualified Individual, Qualified Employer, or Qualified Employee, and (if applicable) their legal or Authorized Representatives, or any individual who presents himself or herself for assistance related to an Authorized Function from a Non-Exchange Entity, or who is offered assistance related to an Authorized Function by a Non-Exchange Entity, as applicable.

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

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

(15) **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 Non-Exchange Entity privacy notice statement required by Section (1) of Appendix A of the Agreement that incorporates this Appendix B, responsible for the development and implementation of the privacy and security policies and procedures of the Non-Exchange Entity, and responsible for ensuring the NonExchange Entity has in place appropriate safeguards to protect the privacy and security of
PII.

(16) **Downstream Entity** means any party that enters into an agreement with CDO or with another Downstream Entity for purposes of providing services related to the agreement between CDO and CMS. The term "downstream entity" is intended to reach the entity that directly provides services to Consumers.

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

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

(19) **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.

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

(21) **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.

(22) **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.

(23) **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.

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

(25) **Nominal Value** means having a cash value of $15 of less, or having worth of $15 or less, based on the retail purchase price of the item, regardless of the actual cost.

(26) **Non-Exchange Entity** has the meaning at 45 CFR 155.260(b), and includes but is not limited to Certified Application Counselor Designated Organizations, and Certified Application Counselors under agreement with a Certified Application Counselor Designated Organization.

(27) **OMB** means the federal government's Office of Management and Budget.

(28) **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.

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

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

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

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

(33) **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.

(34) **State** means the State where the Non-Exchange Entity that is a party to this Agreement is operating.

(35) **State Partnership Exchange (SPE)** means a type of FFE in which a State engages actively with the federal government in the operation of certain aspects of the FFE.

(36) **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.

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

(38) **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 C: Computer Security Incident Report

Date/Time:

Incident Tracking Number		
CMS	**HHS**	**US CERT**

**** = Required information***

Reporting Individual Contact Information			
Name*		**Email***	
Office Number*	**Cell Number**	**Dept/OPDIV***	**UserID**
Name(s) of Dept/OPDIV or individual notified of security incident:			
Dept/OPDIV	**Name/Title**		**Date/Time Notified**

Impacted User Contact Information			
Name*		**Email***	
Office Number*	**Cell Number**	**Dept/OPDIV***	**UserID**

Incident Category			
	PII | PHI | FTI Incident (Section A)		CAT 5 Scans/Probes (*Section H*)
	CAT 0 Exercise/Network Defense Testing (*Section B*)		CAT 6 Investigations (*Section I*)
	CAT 1 Unauthorized Access (*Section C*)		CAT 7 Other (*Section J*)
	CAT 2 Denial of Service (*Section D*)		CAT 8 Lost/Stolen Asset (*Section K*)
	CAT 3 Malicious Code (*Section E*)		CAT 99 Non-Incident (*Section L*)
	CAT 4 Improper Usage (*Section F*)		

Impact Classification*		
Functional Impact		**HIGH** - Organization has lost the ability to provide all citical services to all system users
		MEDIUM - Organization has lost the ability to provide a critical service to a subset of system users.
		LOW - Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
		NONE - Organization has experienced no loss in ability to provide all services to all users.
Information Impact		**CLASSIFIED** - The confidentiality of classified information was compromised.
		PROPRIETARY - The confidentiality of unclassified proprietary information, such as protected critical infrastructure (PCCII), intellectual property, or trade secrets was compromised.
		PRIVACY - The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
		INTEGRITY - The necessary integrity of information was modified without authorization.
		NONE - No information was exfiltrated, modified, deleted, or otherwise compromised.
Recoverabilty		**REGULAR** - Tiem to recovery is predictable with existing resources.
		SUPPLEMENT - Time to recovery is predictable with additional resources.
		EXTENDED - Time to recovery is unpredictable; additional resources and outside help are needed.
		NOT RECOVERABLE - Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
		NOT APPLICABLE - Incident does not require recovery.

Threat Vector Identification*		
Threat Vector		**Description**
	UNKNOWN	Cause of atack is unidentified
	ATTRITION	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks or services
	WEB	An Attack executed from a website or web-based application.
	E-MAIL	An attack executed via e-mail message or attachment.
	EXTERNAL/REMOVABLE MEDIA	An attack executed from removable media or a perifpheral device.
	IMPERSONATION / SPOOFING	An attack involving replacement of legitimate content/services with a malicious substitute.
	IMPROPER USAGE	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above catagories.
	LOSS OR THEFT OF EQUIPMENT	The loss or theft of a computing device or media used by the organization.
	OTHER	An attack does not fit into any other vector.

Section A: PII / PHI / FTI Breach

Breach Category - Check Below			
	Document Theft		Improper Usage
	Hardware / Media Theft		Unintended manual Disclosure
	Document Loss		Unintended Electronic Disclosure
	Hardware / Media Loss		Hacking or IT Incident
	Document Lost in Transit		Document sent to Wrong Address
	Hardware / Media Lost in Transit		

Number and Description of PII / PHI / FTI Lost or Compromised			
List Number Below			
	Exact Number of PII:		Check Here if Number is Unknown:
Brief Description			
Include PII / PHI / FTI format (email, web, database, etc), population effected, lost/stolen, summary time stamp and actions taken.			

Section B: Exercise / Testing (CAT 0)		
Testing Point of Contact		Testing Time Period
Name:		
Phone:		
Brief Description of Test: Including reason for test and networks / systems involved		

Section C: Unauthorized Access (CAT 1)
Describe Violation
Actions Taken (If Any)

Section D: Denial of Service (CAT 2)
Describe Violation
Actions Taken (If Any)

Section E: Malicious Code (CAT 3)			
Malware Type		Malware Name (if Known)	
	Worm		
	Virus	Action Taken	
	Trojan		Quarantined
	Buffer Overflow		Cleaned
	Denial of Service		No Action
	Other	Forensic Image Taken	
		Yes	No
Describe Violation			
Actions Taken (If Any)			

Section F: Improper Usage (CAT 4)	
Type of Violation	
	(P2P) File Sharing
	Instant Messenger
	Inappropriate Web Site
	Remote Access
	Unapproved Software
	Other
Describe Violation	

Section H: Scans / Probes / Attempted Access (CAT 5)		
Timeframe of Activity	Date:	Time:
Source IP / Subnet	Source Port(s)	
Destination IP / Subnet	Destination Port(s)	
Description of Activity		
Actions Taken		

Section I: Investigation (CAT 6)

Timeframe of Activity	Date:	Time:
Detailed Description of Activity		
Actions Taken		

Section I: Other (CAT 7)		
Timeframe of Activity	Date:	Time:
Description		

Section H: Lost / Stolen Asset (CAT 8)			
Device / Media / Object Type			
	Cell Phone		PDA
	Computer (Non-Specific)		Server
	Computer Files		Tape / DLT / DASD
	Desktop Computer		USB Thumb Drive
	E-mail		Other
	Hard Drive (External)		Laptop
	hard Drive (Internal)		Paper Documents

Description
Actions Taken

Section I: Non-Incident (CAT 99)
Detailed Description of Activity
Actions Taken