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/or CAC must permit the Consumer to revoke the authorization at any time.

(b) Informed Consent:

i. CDO and/or 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/or 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 Section (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, addresses, tax filing status, income and deductions, access to employer-sponsored 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/or 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 and 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 and 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-Information-Technology/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/CMS-Information-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's and 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 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 and/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.