***Please note: The excerpts provided below were included as attachments to the Terms and Conditions received by Navigator grantees in 2014 as part of their Notice of Award and are meant to serve as an example only. The standards for 2015 Navigator grantees may be different.**

Notice of Award: Standard Grant/Cooperative Agreement Terms and Conditions (from Attachment A)

16. Project and Data Integrity. Recipient shall protect the confidentiality of all project-related information that includes personally identifying information.

The Recipient shall assume responsibility for the accuracy and completeness of the information contained in all technical documents and reports submitted. The CMS Project Officer shall not direct the interpretation of the data used in preparing these documents or reports.

At any phase in the project, including the project's conclusion, the Recipient, if so requested by the CMS Project Officer, must deliver to CMS materials, systems, or other items used, developed, refined or enhanced in the course of or under the award. The Recipient agrees that CMS shall have a royalty-free, nonexclusive and irrevocable license to reproduce, publish, or otherwise use and authorize others to use the items for Federal government purposes.

Notice of Award: Program Terms & Conditions (from Attachment D)

17. Privacy and Security Compliance.

Definitions. Capitalized terms not otherwise specifically defined in this specific term and condition shall have the meaning set forth in Attachment F.

Authorized Functions. Recipient may collect, handle, disclose, access, maintain, store, and/or use PII of Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or from these individuals' legal representative(s) or Authorized Representative(s), only to perform:

a. the required duties described in section 1311(i)(3) of the Affordable Care Act, 45 CFR 155.210(e), the Cooperative Agreement to Support Navigators in Federally-Facilitated and State Partnership Marketplaces Funding Opportunity Announcement ("Navigator

FOA"), and 45 CFR 155.215(a)(1)(iii), as well as in Recipient's approved work and project plans; or

b. 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) Recipient notifies Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or these individuals' legal representative(s) or Authorized Representative(s), 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. Recipient should provide the required notification through the authorization obtained in accordance with 45 CFR 155.210(e)(6).

The required duties that will most likely involve the collection, handling, disclosure, access, maintenance, storage and/or use of PII of Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or from these individuals' legal representatives(s) or Authorized Representatives, include the following:

- Provide information and services in a fair, accurate, and impartial manner, which includes: providing 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. Such information must acknowledge other health programs such as Medicaid and CHIP;
- Facilitate selection of a QHP;
- Provide referrals to any applicable office of health insurance consumer assistance or health insurance ombudsman established under Section 2793 of the PHS Act, or any other appropriate State agency or agencies, for any enrollee with a grievance, complaint, or question regarding their health plan, coverage, or a determination under such plan or coverage;
- Provide information in a manner that is culturally and linguistically appropriate to the needs of the population being served by the Exchange, including individuals with limited English proficiency, and ensure accessibility and usability of Navigator tools and functions for individuals with disabilities in accordance with the Americans with Disabilities Act and Section 504 of the Rehabilitation Act;
- Comply with the authorization requirements set forth in 45 CFR 155.210(e)(6) and summarized below; and
- Provide information to consumers about the full range of QHP options and insurance affordability programs for which they are eligible, in accordance with 155.215(a)(1)(iii).

Such information may not be reused for any other purpose except as provided in Section 17.b of this Attachment or as otherwise authorized by HHS.

Other Required Duties: Recipient must also maintain expertise in eligibility, enrollment, and program specifications and conduct public education activities to raise awareness about the

Exchange; however, it is not expected or required that Recipient collect, handle, disclose, access, maintain, store and/or use PII of Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or from these individuals' legal representatives(s) or Authorized Representatives for this function. To the extent that Recipient does so, it must comply with all of the provisions of this specific term and condition, as well as Attachments E and F that apply to Recipient's activities.

PII Received. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, Recipient may create, collect, disclose, access, maintain, store, and/or use the following PII from Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or from 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 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 status indicator
PII related to any enrollee with a grievance, complaint, or question regarding their health plan, coverage, or a determination as described in 45 CFR §155.210(e)(4)
Special enrollment period reason
Subscriber Indicator and relationship to subscriber
Social Security Number
Tobacco use indicator and last date of tobacco

Storing PII. Recipient is not expected or required to maintain or store any of the above listed PII as a result of carrying out the Authorized Functions described above or any other required duties, other than in connection with the storage of records of authorizations required by these terms and conditions, and/or as required by 45 CFR 155.210(e)(6). To the extent that Recipient does maintain or store PII, it must comply with all of the provisions of this specific term and condition and Attachments E and F that address maintenance or storage of PII, and with relevant provisions of the Minimum Acceptable Risk Standards for Exchanges specifically referenced below.

Privacy and Security Obligations of Recipient. As a condition of this grant, Recipient will implement and comply with all Exchange privacy and security standards set forth in this specific term and condition as well as Attachments E and F, and the Minimum Acceptable Risk Standards for Exchanges (MARS-E) Version 1.0, which is available at http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/index.html#MinimumAcceptableRiskStandards, and with the Minimum Acceptable Risk Standards for Exchanges Version 2.0, when it is effective.

Authorization Requirement. Prior to collecting any PII, Recipient must obtain the authorization of Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees or these individuals' legal representative(s) or Authorized Representative(s), in accordance with 45 CFR 155.210(e)(6), to ensure that Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees or these individuals' legal representative(s) or Authorized Representative(s):

- are informed of the functions and responsibilities of Navigators;
- provide authorization in a form and manner deemed acceptable by CMS prior to a Navigator's obtaining access to their PII, and that the Navigator maintains a record of the authorization provided in a form and manner deemed acceptable by CMS, for

no less than six years, unless a different and longer retention period has already been provided under other applicable Federal law; and

- may revoke at any time such authorization provided the Navigator.

A template authorization form developed by CMS will be provided separately to all Recipients.

Applicability to Workforce. Recipient must impose the same standards described in this specific term and condition and in Attachments E and F on all Workforce members working with the Recipient on this grant program.

Survival. Recipient covenants and agrees to destroy all PII of Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or those individuals' legal representatives or Authorized Representatives in its possession at the end of the record retention period required under this specific term and condition and Attachments E and F. If, upon the termination or expiration of this grant, the Navigator has in its possession PII for which no retention period is specified in this specific term and condition and/or Attachments E and F, such PII shall be destroyed within 30 Days of the termination or expiration of this grant. Recipient's duty to protect and maintain the privacy and security of PII, as provided for in accordance with this specific term and condition, and Attachments E and F, shall continue in full force and effect until such PII is destroyed and shall survive the termination or withdrawal of the Navigator Recipient and/or expiration of this Agreement.

Notice of Award: Program Terms and Conditions
(Attachment E)

PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS FOR NON-EXCHANGE[1] 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. All terms used herein carry the meanings assigned in Version 1 of Attachment F, which is also attached to this Notice of Award.

The standards and implementation specifications that are set forth in this Attachment E and the Minimum Acceptable Risk Standards for Exchanges (MARS-E) Version 1.0, which is available at http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/index.html#MinimumAcceptableRiskStandards, and with the Minimum Acceptable Risk Standards for Exchanges Version 2.0, when it is effective,
are the same as, or more stringent than, the privacy and security standards and implementation specifications that we have established for the Federally-Facilitated Exchanges ("FFEs") under Section 1321(c) of the Affordable Care Act (42 U.S.C. § 18041(c)).

The FFEs will enter into contracts or grants, such as this Notice of Award (hereinafter "Agreement" or "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, or these individuals' legal representatives or Authorized Representatives. That Agreement and its appendices, including this Attachment E, govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by Non-Exchange Entities in the context of the FFE. In signing that Agreement, in which this Attachment E has been incorporated, Non-Exchange Entities agree 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 their respective Agreements.

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

[1] For purposes of this attachment, the term "Exchange" is used instead of "Marketplace" (see footnote 1).

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, or these individuals' legal representatives and Authorized Representatives, with a simple and timely means of appropriately accessing PII pertaining to them and/or the person they represent in a physical or electronic readable form and format.*

a. Standard: 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, or these individuals' legal representatives or Authorized Representatives should generally be required to specify which PII he or she would like access to. The Non-Exchange Entity may assist them in determining their Information or data needs if such assistance is requested.
5. Subject to paragraphs (1)a.i.6 and 7 below, Non-Exchange Entities generally must provide access to the PII in the form or format requested, if it is readily producible in such form or format.
6. The Non-Exchange Entity may charge a fee only to recoup their costs for labor for copying the PII, supplies for creating a paper copy or a copy on electronic media, postage if the PII is mailed, or any costs for preparing an explanation or summary of the PII if the 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.

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 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 representatives or Authorized Representatives, are provided a reasonable opportunity and capability to make informed decisions about the creation, collection, disclosure, access, maintenance, storage, and use of their PII.*

a. Standard: Informed Consent. The Non-Exchange Entity may create, collect, disclose, access, maintain, store, and use PII from Consumers, Applicants, Qualified Individuals, Enrollees, or these individuals' legal representatives or Authorized Representatives, only for the functions and purposes listed in the Privacy Notice Statement and any relevant agreements in effect as of the time the information is collected, unless the FFE 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 Agreement and any appendices. Such information shall never be used to discriminate against a Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, or Qualified Employer.*

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 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 representatives or Authorized Representatives, an opportunity to request amendment, correction, substitution, or deletion of PII maintained and/or stored by the Non-Exchange Entity if such individual believes that the PII is not accurate, timely, complete, relevant, or necessary to accomplish an Exchange-related function, except where the 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, or these individuals' legal representatives or Authorized Representatives, on their request per the procedures outlined under the access standards in Section (1) above.

(6) *Accountability. In keeping with the standards and implementation specifications used by the FFE, 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[2] 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 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.

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

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.

Notice of Award: Program Terms and Conditions
(Attachment F)

DEFINITIONS

This Attachment defines terms that are used in the Notice of Award, Attachments D, E, and F.

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

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

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

(10) **CMS 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.

(11) **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 APTCs and CSRs, and/or completing enrollment in a QHP through its web site for individual market coverage.

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

(13) **Day or Days** means calendar days unless otherwise expressly indicated in the relevant provision of the Notice of Award terms and conditions that incorporates this Attachment F.

(14) **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.

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

(16) **Exchange** (or **Marketplace**) has the meaning set forth in 45 CFR 155.20.[3]

(17) **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.

(18) **Health Insurance Coverage** has the meaning set forth in 45 CFR 155.20.

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

(20) **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.

(21) **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.

[3] In this attachment, the terms "Exchange" and "Marketplace" are both used to refer to the American Health Benefit Exchanges that are described at Affordable Care Act section 1311(b) and defined at 45 C.F.R. §155.20 (see footnote 1).

(22) **Issuer** has the meaning set forth in 45 CFR 144.103.

(23) **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.

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

(25) **Non-Exchange Entity** has the meaning at 45 CFR 155.260(b), and includes but is not limited to Navigators.

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

(27) **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.

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

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

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

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

(32) **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.

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.

(33) **State** means the State where the Navigator that is a party to the Notice of Award is operating.

(34) **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.

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

(36) **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.

(37) **Workforce** means a Non-Exchange Entity's or FFE's employees, agents, contractors, subcontractors, officers, directors, agents, representatives, volunteers and any other individual who may create, collect, disclose, access, maintain, store, or use PII in the performance of his or her duties.