

# EXAMPLE Privacy and Security Standards

*\*Please note: The privacy and security excerpts provided below are similar to those that were included in the 2023-2024 Terms and Conditions received by Navigator awardees as part of their Notice of Award and serve as an example only. The standards for any future Navigator awardees may be different.*

---

## Standard Grant/Cooperative Agreement Terms and Conditions

### 27. Reporting Requirements.

#### A. PROJECT DATA AND INTEGRITY

Recipient shall protect the confidentiality of all project-related information that includes personally identifying information (PII).

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.

---

## Program Terms & Conditions: Attachment H

### 8. Navigator Oversight and Monitoring.

- Recipient shall establish processes to monitor program activities for compliance with statutory, regulatory, and cooperative agreement requirements, including but not limited to compliance with the privacy and security requirements set forth in this document (*Attachments H-J, Program Terms and Conditions*).
- Recipient is required to report to CMS any instance of suspected fraud, misconduct or non-compliance with statutory, regulatory or cooperative agreement requirements on the part of paid and unpaid workforce and, if applicable,

contracted entities (regardless if contracted for Navigator duties or other purposes such as IT or marketing, for example), or the organization as a whole.

- Recipient should make contact information for the HHS Office of Inspector general (OIG) available to Consumers and to Recipient paid and unpaid workforce. For example, this could be done by posting this information in a public space or by including in educational materials distributed by Recipient.

## **16. 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 J*.

Recipient hereby acknowledges and agrees to accept and abide by the standards and implementation specifications set forth in this document (*Attachment H*, Program Terms and Conditions) and in *Attachment I* (Privacy and Security Standards for Navigator Cooperative Agreement Recipients) when engaging in any Navigator Authorized Functions as defined below. Recipient is thereby bound to strictly adhere to the privacy and security standards, and to ensure that its Workforce that creates, collects, handles, discloses, accesses, maintains, stores, and/or uses PII of Consumers, is contractually bound to strictly adhere to those standards and implementation specifications.

Navigator Authorized Functions. Recipient may create, collect, handle, disclose, access, maintain, store, and/or use PII of Consumers, only to perform:

- a. the required duties described in section 1311(i)(3) of the Affordable Care Act, 45 C.F.R. §§ 155.210 and 155.215, and the Cooperative Agreement to Support Navigators in Federally-Facilitated Exchanges Notice of Funding Opportunity Announcement (NOFO, or Funding Opportunity), as well as in Recipient's approved work and project plans;
- 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 ACA within the meaning of section 1321(d) of the ACA, and (2) Recipient notifies Consumers, in advance, in writing, that creation, 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 C.F.R. § 155.210(e)(6); and
- c. other functions authorized under 45 C.F.R. §§ 155.210 and 155.215, and such other functions that may be approved by CMS in writing from time to time.

The required duties that are most likely to involve the creation, collection, handling, disclosure, access, maintenance, storage and/or use of PII of Consumers 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 qualified health plans (QHPs); and helping consumers make informed decisions during the health coverage selection process. Such information must acknowledge other health programs;
- 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 Exchanges, 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 C.F.R. § 155.210(e)(6) and summarized below;
- Provide targeted assistance to serve underserved or vulnerable populations, as identified by the Exchange, within the Exchange service area; and
- Provide information to Consumers about the full range of QHP options and insurance affordability programs for which they are eligible, in accordance with 45 C.F.R. § 155.215(a)(1)(iii).

Use of Data in the Marketplace Assister Community (MAC): See *Attachment I*, Item (13) for the specific requirements Recipient and Recipient's workforce must adhere to when accessing, managing, or using consumer PII in the MAC.

Other Required Duties: Recipient must also maintain expertise in eligibility, enrollment, and program specifications and conduct public education activities to raise awareness about the Exchanges; however, it is not expected or required that Recipient create, collect, handle, disclose, access, maintain, store and/or use PII of Consumers 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 H, I, and J* that apply to Recipient's activities.

PII Received. Subject to these terms and conditions of this Notice of Award and applicable laws, in performing the tasks contemplated under this award, Recipient may create, collect, handle, disclose, access, maintain, store, and/or use PII of Consumers, including but not limited to the following:

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, start and end dates  
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  
Premium Amount, start and end dates  
Pregnancy indicator  
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

Storing PII. To the extent that Recipient maintains or stores PII, it must agree to comply with all provisions of these terms and conditions that apply to the maintenance or storage of PII as outlined in *Attachment I*.

Privacy and Security Obligations of Recipient. As a condition of this cooperative agreement, Recipient will implement and comply with all FFE privacy and security standards set forth in these terms and conditions and throughout all aspects of the cooperative agreement period of performance as outlined in *Attachment I*.

Authorization Requirement. Prior to creating, collecting, handling, disclosing, accessing, maintaining, storing, and/or using any PII from Consumers, Recipient must obtain the authorization required under 45 C.F.R. § 155.210(e)(6), to ensure that Consumers:

- are informed of the functions and responsibilities of Navigators, including that Navigators are not acting as tax advisers or attorneys when providing assistance as Navigators and cannot provide tax or legal advice within their capacity as Navigators;
- provide authorization in a form and manner as determined 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 as determined 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 this authorization at any time.

A model template authorization form developed by CMS will be provided separately to all Recipients for their optional use.

This authorization is separate and distinct from any informed consent obtained pursuant to section 2(b) of *Attachment I* of this Agreement. Recipient should ensure that a record of the authorization provided is maintained in a manner consistent with the privacy and security standards set forth in this document (*Attachment H, Program Terms and Conditions*) and in *Attachment I*.

Collection of PII. Except for collections, uses or disclosures that are specifically authorized by Consumers in accordance with Section 2(b) of *Attachment I*, PII collected from Consumers may be used only for the Navigator Authorized Functions specified in this term and condition.

Ability of Consumer to Limit Collection and Use. Recipient agrees to allow the Consumer to limit the Recipient's creation, collection, handling, disclosure, access, maintenance, storage, and usage of their PII to the sole purpose of obtaining Recipient's assistance for Federally-facilitated Exchanges purposes, and for performing Navigator Authorized Functions specified in this term and condition.

Applicability to Workforce. Recipient must impose the same standards described in this specific term and condition and in *Attachment I* on all Workforce members working with the Recipient on this cooperative agreement program.

Survival. Recipient covenants and agrees to destroy, unless otherwise required by law, all PII of Consumers in its possession at the end of the record retention period required under this specific term and condition and in *Attachments H and I*. 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 H and I*, 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 award.

**17. Sub-Recipients' Compliance with Privacy and Security Requirements.** Recipients are required to bind any and all Sub-Recipients to all privacy and security requirements outlined in this document (*Attachment H, Program Terms and Conditions*) and in *Attachment I*.

**20. PII Authorization.** Recipient may not create, collect, handle, disclose, access, maintain, store, and/or use the PII (as defined in *Attachment J*) of any Consumers until it has drawn down funds and in doing so, has accepted the terms and conditions of this award.

# Program Terms and Conditions: Attachment I

## **PRIVACY AND SECURITY STANDARDS FOR NAVIGATOR COOPERATIVE AGREEMENT RECIPIENTS**

These standards and implementation specifications are established in accordance with Section 1411(g) of the Affordable Care Act (ACA) (42 U.S.C. § 18081(g)) and 45 C.F.R. § 155.260. As used in this Attachment, all terms used herein carry the meanings assigned in *Attachment J* of the Notice of Award.

A Navigator Cooperative Agreement Recipient (“Recipient”), and any members of Recipient’s Workforce who are certified by CMS to carry out Navigator duties, or who otherwise have access to the PII of Consumers who seek the Recipient’s assistance, must adhere to the following privacy and security standards and implementation specifications in performing the Navigator Authorized Functions defined in *Attachment H* of the Notice of Award.

- (1) Privacy Notice Statement. Prior to collecting PII or other information from Consumers for the purpose of fulfilling a Navigator Authorized Function, Recipient 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 or paper form the Recipient will use to gather or request PII from Consumers. The privacy notice statement must also be prominently and conspicuously displayed on the Recipient’s public facing Web site, if applicable, if the Recipient will gather or request PII 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 Recipient;

5. What, if any, notice or opportunities for consent will be provided regarding the creation, collection, handling, disclosure, access, maintenance, storage, and/or use of the information;
  6. How the information will be secured while in the possession of Recipient or its Workforce or agents (Sub-Recipients);
  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 Recipient related to the Recipient's activities in relation to the information collected.
- iii. The Recipient 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 from Consumers, this provision does not require Recipients 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 Navigator Authorized Function or sending to the consumer educational information that is directly relevant to Navigator Authorized Functions. Nonetheless, with regard to such names, physical addresses, e-mail addresses, or telephone numbers, Recipients still must comply with all other privacy and security standards and requirements outlined in the CMS Navigator Cooperative Agreement Terms and Conditions.
- (2) Permissible Uses and Disclosures of PII. The Recipient and members of Recipient's Workforce who are certified by CMS to carry out Navigator duties may create, collect, handle, disclose, access, maintain, store, and/or use PII of Consumers only for Navigator Authorized Functions identified in *Attachment H*, unless the Recipient obtains informed consent as described in Section 2(b) of this *Attachment I*.



a. Authorization:

- i. Prior to creating, collecting, handling, disclosing, accessing, maintaining, storing, or using any Consumer PII to perform a Navigator Authorized Function, the Recipient must obtain the authorization required by 45 C.F.R. § 155.210(e)(6), (hereinafter referred to as “Authorization”). This is separate and distinct from the informed consent referenced in Section 2(b) below;
- ii. Recipients 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 and State laws; and
- iii. Recipients must permit the Consumer to revoke the authorization at any time.

b. Informed Consent:

- i. Recipients must obtain informed consent from Consumers for any creation, collection, handling, disclosure, access, maintenance, storage, and/or use of their PII that is not authorized under these Terms and Conditions. Such informed consent must be in writing, signed by the consenting party, and subject to a right of revocation.
- ii. Recipients are prohibited from denying information or assistance described in the Navigator Program Terms and Condition to persons or entities who decline to grant the informed consent described in section 2(b)(i) above.
- 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 Recipient 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 and State laws.

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

- a. Permissible creation and use of PII.

Other than in accordance with the informed consent procedures outlined in section 2(b) above, the Recipient shall only create, collect, handle, disclose, access, maintain, store, or use PII it receives in its capacity as a Navigator Grant Recipient:

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

- b. Prohibited requests for, collections, or uses of PII.

The Recipient **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. § 155.731. Such necessary information may include information about an individual who lives with or shares a tax household with the individual seeking coverage, such as contact information, addresses, tax filing status, income and deductions, access to employer-sponsored coverage, familial or legal relationship, 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 Navigator Authorized Functions, Recipients that maintain 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. Recipients 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, a Recipient is required to establish and implement operational, technical, administrative, and physical safeguards that are consistent with any applicable laws to ensure that PII is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information. Such safeguards must include:
  - i. Email/Web Browser Protections—including, but not limited to, assuring that transfer protocols are secure and limit the threat of communications being intercepted.
  - ii. Endpoint Protection and Network Management—including, but not limited to, protecting against known threat vectors within the system's environment to mitigate damage and security breaches.
  - iii. Access Management—including, but not limited to, managing access to the system's environment and data, and maintaining access controls to the system.
  - iv. Asset Management—including, but not limited to, maintaining an inventory of hardware and software within the environment to help identify vulnerable aspects left open to threat vectors without performing vulnerability scans, and maintaining specific knowledge of physical and digital assets within the system's environment.

- v. Configuration Management—including, but not limited to, managing baseline configurations of system servers and endpoints to mitigate threat factors that can be utilized to gain access to the system and data.
  - vi. Vulnerability Management—including, but not limited to, identifying, classifying, remediating, and mitigating vulnerabilities on a continual basis by conducting periodic vulnerability scans to identify weaknesses within an environment.
  - vii. Patch Management—including, but not limited to, ensuring every client and server is up to date with the latest security patches throughout the environment.
  - viii. Incident Response—including, but not limited to, detecting security events, investigating, and mitigating or limiting the effects of those events.
  - ix. Governance and Privacy Compliance Program—including, but not limited to, appointing a responsible official to develop and implement operational privacy compliance policies for information systems and databases.
  - x. Privacy Impact/Risk Assessment—including, but not limited to, appointing a responsible official to develop and implement formal policies and procedures to assess the organization’s risk posture.
  - xi. Data Protection and Loss Prevention—including, but not limited to, ensuring that PII is only used by or disclosed to those authorized to receive or view it; PII is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information; and PII is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law.
  - xii. Data Retention and Destruction—including, but not limited to, developing formal policy and procedures for data retention and destruction of PII consistent with CMS and the Exchange system requirements.
- b. Recipient must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls.
  - c. Recipient must develop, and Recipient and any members of Recipient’s Workforce who are certified by CMS to carry out Navigator duties must utilize, secure electronic interfaces when transmitting PII electronically.

(5) Incident and Breach Reporting Requirements.

- a. Reporting. Recipients must implement and comply with Breach and Incident handling procedures that are consistent with CMS' current edition of the Risk Management Handbook (RMH) for Incident Management.<sup>1</sup> Such policies and procedures must be documented in writing in Recipient's own policies and procedures, and:
  - i. Identify the Recipient's Designated Privacy Official, or, if applicable, 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 members of Recipient's Workforce to report all potential Incidents or Breaches to Recipient;
  - 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 to [cms\\_it\\_service\\_desk@cms.hhs.gov](mailto:cms_it_service_desk@cms.hhs.gov) within 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches, but within 72 hours from knowledge of the Incident;
  - vi. Provide details regarding the identification, response, notification, mitigations, recovery, after-action, and follow-up of Incidents and Breaches; and
  - vii. Require the Recipient's Designated Privacy Official or other personnel authorized to be available to CMS upon request.
- b. Members of Recipient's Workforce must comply with Navigator Awardee Organization's Breach and Incident handling procedures.
- c. Cooperation. Recipients 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 Recipient shall develop role-based training and awareness programs for members of its Workforce who are certified by CMS to

---

<sup>1</sup> Available at <https://security.cms.gov/policy-guidance/cms-breach-response-handbook>.

carry out Navigator duties or who otherwise have access to the PII of consumers who seek the Recipient's assistance. Recipient shall require such members of its Workforce to participate in such training and awareness programs. Specifically, the Recipient must require such 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 prior to having access to PII.

- (7) Standard Operating Procedures Requirements. The Recipient shall incorporate the privacy and security standards and implementation specifications required under this *Attachment I*, where appropriate, in its standard operating procedures that are associated with the functions authorized under Navigator Terms and Conditions involving the creation, collection, handling, disclosure, access, maintenance, storage, and/or use of PII. Members of Recipient's Workforce whether paid or unpaid and who are certified by CMS to carry out Navigator duties, or who otherwise have access to the PII of consumers who seek the Recipient's assistance, must comply with these standard operating procedures. The Recipient's standard operating procedures:
- a. Must be written in plain language and be available to all of the Recipient's Workforce;
  - b. Must ensure the Recipient'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 Navigator Terms and Conditions; 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 Recipient 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 Recipient, to ensure such compliance.
- (8) Required Monitoring of Privacy and Security Controls. Recipient must monitor, periodically assess, and update its privacy and security controls and related system risks to ensure the continued effectiveness of those controls.
- (9) Required Flow-Down of Privacy and Security Agreements. Recipient must bind, in a signed writing, any members of Recipient's Workforce who are certified by CMS to carry out Navigator duties, and any Downstream Entities to the same privacy and security standards and obligations contained in this *Attachment I*.

- (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 Recipient, 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. Recipient acknowledges that any person who knowingly and willfully uses or discloses information in violation of section 1411(g) or 1411(h) of the ACA 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.
- (12) Access to the FFEs and SBE-FPs. Recipient, and all members of its Workforce, are prohibited from remotely connecting or transmitting data to the FFE, SBE-FP, or their testing environments, or remotely connecting or transmitting data to IT systems that maintain connections to the FFE, SBE-FP, or their testing environments, from locations outside of the United States of America, its territories, embassies, or military installations. This includes any such connection through virtual private networks (“VPNs”).
- (13) Use of Data in the Marketplace Assister Community (MAC). To keep people enrolled in coverage during the COVID-19 Public Health Emergency (PHE), under what is known as the “continuous enrollment condition,” states paused terminations for Medicaid (and in some cases, Children's Health Insurance Program (CHIP)) coverage, starting in March 2020. This condition meant that, with limited exceptions, consumers who were enrolled in Medicaid and became ineligible for that coverage would not lose Medicaid until the end of the quarter in which the COVID-19 Public Health Emergency (PHE) ended.

Some states adopted similar flexibilities for CHIP in their respective states. Although the continuous enrollment condition was originally linked to the COVID-19 PHE, on December 29, 2022, the [Consolidated Appropriations Act, 2023](#) (CAA, 2023), separated the continuous enrollment condition from the end of the COVID-19 PHE.

The CAA, 2023, designated March 31, 2023, as the end of the Medicaid continuous enrollment condition. Now that the condition has ended, states are required to resume regular eligibility and enrollment operations, including renewals and coverage terminations. This process is referred to as “Medicaid unwinding.” States must initiate eligibility renewals within 12 months for all individuals enrolled as of March 31, 2023, and must complete eligibility renewals within 14 months for individuals enrolled as of March 31, 2023. The first date that states could terminate Medicaid was April 1, 2023, for consumers found ineligible for that coverage. In some states, renewals began as

early as February 1, with the first terminations effective on April 1. The anticipated start dates for each state's redeterminations can be found on [Medicaid.gov](https://www.Medicaid.gov).

There are a number of challenges Medicaid/CHIP enrollees could face as eligibility redeterminations begin, and millions of people will lose their coverage as a result. To help consumers who will lose their Medicaid/CHIP coverage transition to other coverage options, such as the Marketplace, CMS is expanding its direct assister-to-consumer outreach program that was piloted during the 2023 Marketplace Open Enrollment Period. States are required to securely send account information to CMS for consumers whose Medicaid/CHIP coverage has been or will be terminated, and that information is being shared with Navigators who have been trained to conduct direct outreach through the Marketplace Assister Community (MAC).

Only Navigator Cooperative Agreement Recipients authorized by CMS, who have been trained and certified by the FFE (as outlined in *Attachment H, Item 9. Navigator Training Requirements*), and who have completed the CMS-approved MAC trainings can access the MAC. Recipient, including all of its workforce and subrecipients/sub-awardees and any contractors, must adhere to the following guidelines in addition to all other Consumer PII requirements in these terms and conditions. **Failure to do so will result in disciplinary and corrective actions as determined by CMS.**

***Prohibitions for all MAC Users:***

- Access, manage, or use consumer PII in the MAC for purposes other than conducting outreach in order to help the consumer and members of their household understand the coverage options available to them.
- Save or manage consumer PII or interactions outside of the MAC.
- Save or manage consumer PII on any device (computer, tablet, phone, etc.) with an internet connection unless it's essential for conducting your business and kept in accordance with the Navigator Terms and Conditions.
- Attempt to speak with minors about their coverage.
  - In the event a minor is reached at a phone number provided for an adult, ask to speak to the head of household or other adult and note any contact information errors in the touchpoint form in the MAC.



**Effective June 18, 2023**, outreach and education activities may be conducted by going door-to-door or through other unsolicited means of direct contact, including calling a Consumer, to provide application or enrollment assistance.<sup>2</sup>

---

<sup>2</sup> See the HHS Notice of Benefit and Payment Parameters for 2024 final rule at <https://www.federalregister.gov/d/2023-08368/p-142> which removed the prohibition, on Navigators, non-Navigator assistance personnel, certified application counselors (CACs), and CAC Designated Organizations (CDOs) in FFEs going door-to-door or using unsolicited means of direct contact to provide application or enrollment assistance.

## Program Terms and Conditions: Attachment I

*This Attachment defines terms that are used in Attachments H, I, and J.*

### **DEFINITIONS**

- (1) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 C.F.R. § 155.20.
- (2) **Affordable Care Act (ACA) of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152).**
- (3) **Applicant** has the meaning set forth in 45 C.F.R. § 155.20.
- (4) **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 these Terms and Conditions.
- (5) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 C.F.R. § 155.227.
- (6) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for anything other than an authorized purpose.
- (7) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (CMS).
- (8) **CMS** means the Centers for Medicare & Medicaid Services.
- (9) **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.
- (10) **Cost-sharing Reduction (CSR)** has the meaning set forth in 45 C.F.R. § 155.20.
- (11) **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 *Attachment I*, responsible for the development and implementation of the

privacy and security policies and procedures of the Non-Exchange Entity, and responsible for ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy and security of PII.

- (12) **Downstream Entity** means any party that enters into an agreement with Recipient or with another Downstream Entity for purposes of providing services related to the Navigator grant. The term “downstream entity” is intended to reach the entity that directly provides services to Consumers.
- (13) **Enrollee** has the meaning set forth in 45 C.F.R. § 155.20.
- (14) **Exchange** has the meaning set forth in 45 C.F.R. § 155.20. The term Exchange, and the term “Marketplace” are commonly used to refer to the American Health Benefit Exchanges that are described at Patient Protection and Affordable Care Act section 1311(b) and defined at 45 C.F.R. § 155.20.
- (15) **Federally-facilitated Exchange (FFE)** means an Exchange 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).
- (16) **HHS** means the U.S. Department of Health & Human Services.
- (17) **Incident, or Security Incident**, has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- (18) **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.
- (19) **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 Patient Protection and Affordable Care Act.
- (20) **Marketplace Assister Community (MAC)** is a secure, online platform leveraged by Navigators in the Federally-facilitated Marketplace (FFM). Consumers whose Medicaid or CHIP coverage has been or will be terminated are assigned to the MAC for outreach. Through the MAC, CMS assigns consumers to a Navigator organization for outreach and enrollment assistance based on the consumer's proximity to the organization and the availability and capacity of the organization to provide enrollment assistance. Navigators use the MAC to manage their consumer assignments, as well as document consumer interactions and enrollment assistance outcomes.
- (21) **Navigator** has the meaning set forth in 45 C.F.R. § 155.20.
- (22) **Non-Exchange Entity** has the meaning at 45 C.F.R. § 155.260(b) and includes but is not limited to Navigator award recipients, and their paid and unpaid staff who are certified by CMS to carry out Navigator duties.
- (23) **OMB** means the federal government's Office of Management and Budget.
- (24) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- (25) **Qualified Employee** has the meaning set forth in 45 C.F.R. § 155.20.
- (26) **Qualified Employer** has the meaning set forth in 45 C.F.R. § 155.20.
- (27) **Qualified Health Plan (QHP)** has the meaning set forth in 45 C.F.R. § 155.20.
- (28) **Qualified Individual** has the meaning set forth in 45 C.F.R. § 155.20.
- (29) **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.
- (30) **Subaward** means an award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

- (31) **Subrecipient** means a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency. For purposes of these terms and conditions, subgrantee/subawardee and subrecipient retain the same meaning.
- (32) **Web** means the World Wide Web.
- (33) **Workforce** means a Non-Exchange Entity's or subrecipients' employees, agents, contractors, subcontractors, officers, directors, agents, representatives, and any other individual who may create, collect, handle, disclose, access, maintain, store, and/or use PII in the performance of their duties.