Best Practices for Handling Personally Identifiable Information: Fast Facts for Assisters

Updated February 2015

This Fact Sheet Applies If You:

- Are a Navigator, non-Navigator assistance personnel ("in-person assister"), or certified application counselor (collectively, an assister) in a state with a Federally-facilitated Marketplace or State Partnership Marketplace
- Have questions about personally identifiable information (PII)
- Are looking for best practices and tips on handling PII

Personally Identifiable Information (PII): Overview

As a Navigator, non-Navigator assistance personnel (or "in-person assister"), or certified application counselor (CAC) (collectively referred to as an "assister") helping consumers who are applying for health insurance through a Federally-facilitated or State Partnership Marketplace, you may encounter consumers' personally identifiable information (PII). This document contains suggested measures to take for protecting consumers' personally identifiable information (PII) in the course of performing assister duties. Remember: *these suggestions are not intended to replace your obligation to determine how to follow the specific privacy and security standards that apply to your work, and the suggestions in this document might not be necessary in all circumstances, or you might have to do more than what is suggested here in order to meet the privacy and security standards that apply to your work. The specific privacy and security standards that apply to your work are contained in your organization's agreement with CMS or the terms and conditions for your grant or contract with CMS, as applicable.*

PII is anything that could individually, or in combination with other data elements, identify the consumer, such as a consumer's name, address, telephone number, social security number,

Marketplace application ID or other identifier.[1] Consumers must have an opportunity to access, inspect, and/or correct their PII if they make a request to do so. Only those assisters who need to access or use PII to carry out required duties should be given access to it, and they should access or use only the minimum amount of PII necessary in order to carry out required duties.

Examples:

- Don't request information about a person's status as a citizen, national, or immigrant if that person is not seeking coverage for himself or herself on any eligibility application.
- Don't request an individual's Social Security Number (SSN) if he or she is not seeking coverage for himself or herself, unless information about the individual's income is necessary to determine the applicant's household income. (Note: an individual is not required to provide his or her SSN if he or she is not applying for coverage for himself or herself, but if the individual's income is included in the applicant's household income, providing this information can help speed up the verification process.)
- Don't use someone's PII to discriminate against them, such as by refusing to assist individuals who are older or have significant or complex health care needs.[2]

Protecting consumers' PII should be routinely discussed and monitored within your organization and continuing education is strongly encouraged.

See the list below for examples of PII that you may encounter while assisting consumers. This is not an exhaustive list. If you are a Navigator or certified application counselor, a comprehensive list of types of PII that you might encounter and that you are authorized to access and use is provided in the privacy and security standards that apply to your organization's agreement with CMS or grant terms and conditions, as applicable.

Examples of PII You May Encounter

- Name
- Birth date

---

[1] According to the privacy and security standards set forth in Navigators' grant terms and conditions and certified application counselor organizations' agreements with CMS, PII is defined as "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. (OMB Memoranda M-07-16 (May 22, 2007))."

[2] However, under 45 CFR 155.120(c)(2), CAC organizations that are federally-funded to provide services to a specific population, such as a Ryan White HIV/AIDS program or an Indian health provider, may continue to limit their services to that population, as long as they do not discriminate within that specific population. If CACs providing these limited services are approached by consumers outside of this specific population, they must refer these consumers to Marketplace-approved resources, such as Navigators or other CACs that can provide assistance.

- Social Security number
- Alien Registration Number
- Home address
- Email address
- Phone number
- Electronic or paper federal tax returns (e.g., 1040, 941, 1099, 1120, and W-2)
- Medicaid/CHIP eligibility status
- Citizenship or immigration status
- Applicant ID
- Household income
- Qualified health plan (QHP) eligibility status
- Advanced payments of the premium tax credit/cost-sharing reduction (APTC/CSR) eligibility status
- Spoken and written language preference
- Tobacco usage

One best practice you might want to consider is taking periodic training on the privacy and security requirements that apply to consumer PII during the year, beyond the CMS-required training. This could increase your ability to identify PII and reinforce how to keep consumers' information private and secure.

When Assisters Will Encounter PII

PII is needed and used by the Marketplace to determine or assess consumers' eligibility for health coverage and programs to lower their costs through the Marketplace, as well as to identify available coverage options for all consumers. You might also encounter PII as you help consumers select among various coverage options and enroll in coverage. As you assist consumers who are applying for and enrolling in coverage through the Marketplace, you're likely to encounter PII when assisting consumers with:

- Creating a Marketplace account

- Completing and submitting an application for health coverage
- Assessing options for lowering costs of health coverage
- Selecting and enrolling in a qualified health plan (QHP)
- Applying for an exemption from the individual shared responsibility payment
- Filing an eligibility appeal
- Reporting changes to the Marketplace, including those that may qualify the consumer for a special enrollment period or new eligibility determination

Best Practices related to Obtaining Consumer Authorization (or Consent)

When providing assister services to a consumer for the first time, you should first explain to the consumer your role as an assister and the privacy and security practices that you will take to ensure that the consumer's information is kept private and secure. Once you have discussed this with the consumer, you must obtain the consumer's authorization to provide assistance prior to beginning to obtaining access to the consumer's PII. To help assisters comply with this requirement, CMS has developed a model form that Navigators and CACs may adopt or modify. A revised draft model form was published in November 2014. Records of consumer authorization must be appropriately secured and retained for at least six years, in accordance with federal regulations. Consumers can revoke or limit their authorization at any time.

The following are a few best practices related to the consumer authorization requirement:

- Prior to obtaining access to consumers' PII, develop and follow standard consumer authorization procedures that are appropriate for the nature of your work. For example, if your organization assists individuals over the phone, such procedures might include developing a verbal script and process to document and retain a consumer's oral authorization. CMS provides a model authorization form template for Navigators and CACs to adopt or modify, as appropriate.
- Develop a checklist for assisters to use when providing assistance to a consumer for the first time. This will allow you to be sure all consumers provide their authorization (such as by signing an authorization form or orally consenting) before the session begins.
- Develop a standard operating procedure to document instances where a consumer withdraws or limits their authorization to access their PII.
- Provided the consumer has provided a general authorization to permit you to access his

or her PII to provide assistance, as well as his or her preferred contact information, keep his or her name and contact information to set up appointments or to follow up with the consumer at later date on application or enrollment issues. We recommend as a best practice that preferred contact information be documented at the same time that consumer authorization is obtained, consistent with your organization's standard consumer authorization procedures.

Best Practices related to Providing Application and Enrollment Assistance

- During consumer appointments, utilize private spaces to ensure privacy. If assisters are at an event and a private space is not available, create a space that is out of earshot to discuss private information with potential applicants. Also, use computer screen covers (that are inexpensive to purchase) which can help protect PII from the view of others.
- PII collected from the consumer, including name, email address, telephone number, application ID number, addresses, or other notes must be stored securely.
    - If in hard copy, PII should be stored in locked filing cabinets or within locked offices where the paper filing system is maintained.
    - If in electronic format, PII should be stored securely in a password-protected file on a password-protected computer to which only authorized individuals have access.
- Do not leave files or documents containing PII or tax return information unsecured and unattended on desks, printers, personal computers, phones or other electronic devices, and fax machines.
- Do not send or forward e-mails with PII to personal e-mail accounts (e.g., Yahoo, Gmail).
- Protect e-mails that contain PII (e.g., encryption).
- Do not upload PII to unauthorized websites (e.g., wikis).
- Do not use unauthorized mobile devices to access PII.
- Lock up portable devices (e.g., laptops, cell phones).
- Clear your web browser history to avoid other users accessing PII.
- Disable auto-fill settings on your web browser.

- Keeping notes might be necessary to perform effective application and enrollment assistance for that consumer. For example, a consumer's case may require you to research their specific questions and follow up with them at a later appointment. If a consumer provides a general consent for you to gain access to that consumer's PII to provide assistance, you are permitted to keep notes linked to his or her individual situation, unless the consumer specifically limits his or her consent to prevent you from doing so.

- If you write down any quick notes for your own reference during the phone call with a consumer but do not intend to keep those notes, shred the notes as soon as you complete the call.

- All computer equipment, including mobile devices, should have a password-protected login screen that will not allow access to files without the proper, secure password.

- Any time you step away from a computer, you should lock the computer to avoid the chance that an unauthorized individual gains access to the computer.

- Always return originals or copies of official documents that contain a consumer's PII to consumers and only make copies for yourself or others if necessary to carry out required duties. It can be helpful to have a supply of manila folders to hand to consumers with their documents inside. This helps them keep track of their documents in one place and shields the content of the documents from view.

- If consumers mistakenly or accidentally leave behind PII at a facility or enrollment event, store the documents in a safe, locked location, and return PII to consumers as soon as possible.

- Remind consumers that they should keep their PII locked and in a safe place, or if stored electronically, protected by passwords that they will remember.

What Assisters Need to Know About Breaches and Incidents (this section is focused on Navigators and CACs and the privacy and security standards that apply to their work)

A **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.[3]

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.

You and your organization must implement breach and incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures[4] and memorialized in your organization's own written policies and procedures. Such policies and procedures would:

- Identify your organization'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.
- Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches; and
- Specify adequate procedures by which you can make a reasonable effort to report 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, as required.

Issues you should report include:

- Lost, stolen, or misplaced records containing PII
- Unauthorized personnel seeing or possessing PII
- Lost, stolen, or misplaced electronic devices (e.g., tablets or laptops) that contain consumer PII

Scenarios

1. **Consumer Leaves Behind Documents with PII**: Maggie, a 34-year old single mother, needs help applying for health coverage through the Marketplace. Before she can finish the application, she gets a call from the school's nurse and has to run out quickly when she learns that her son has lice. In her rush to leave, Maggie leaves behind a copy of her

[3] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
[4] Available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_7-1_Incident_Handling_Standard.pdf

tax return with her Social Security number, home address, and phone numbers on the assister's desk. What should the assister do?

The assister should follow Maggie out with the tax return, in the hope that she can catch her and return the papers. In case the assister is unable to find her, the assister should securely store the tax return in a locked drawer until Maggie is able to return and pick up her tax return, or the papers are sent to her home address in a secure, opaque envelope. This would **not** qualify as a breach of PII, and there is no requirement to notify the Marketplace.

2. **Securing PII:** Paul, a 30-year old self-employed carpenter, recently had his credit card information stolen. He is afraid of being a victim of identity theft again. Before signing up for insurance, Paul wants to know how you will safeguard his PII. What should you tell Paul about how PII will be secured?

   Before obtaining access to Paul's PII, you should tell Paul how you work to protect his privacy and the confidentiality of his PII, including telling him what information you might collect, why you might collect it, and how it will be used, as well as whether the information will be shared. Then, Paul must authorize you to access his PII. You should reassure him that you will only access or use the minimum amount of his PII that is necessary to effectively provide assistance for him, keep his PII private and secure at all times, and that he may limit or revoke his authorization to share his PII with you at any time. If Paul brings official documents like his Social Security card that contain his PII when he meets with you, he should take these documents with him when he leaves.

Additional Resources

For More Information Visit:

- Marketplace Privacy and Security Standards
  45 CFR 155.260; any applicable privacy and security standards set forth in agreements, in accordance with §155.26

- Minimum Acceptable Risk Standards for Exchanges (MARS-E)
  Available at: http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/index.html#MinimumAcceptableRiskStandards

- Internal Revenue Service (IRS): Data Safeguards
  IRS Publication 1075 (Jan. 2014), available at: http://www.irs.gov/pub/irs-pdf/p1075.pdf

- OIG Fraud Hotline
  Available at: https://forms.oig.hhs.gov/hotlineoperations

- Federal Trade Commission (FTC): Submission of Fraud Complaint
  Available at: https://www.ftccomplaintassistant.gov/