CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

Assister Guidance: Obtaining Consumer Authorization and Handling Consumers’ Personally Identifiable Information (PII) in the Federally-facilitated Marketplaces (FFMs)

Center for Consumer Information and Insurance Oversight

November 7, 2014

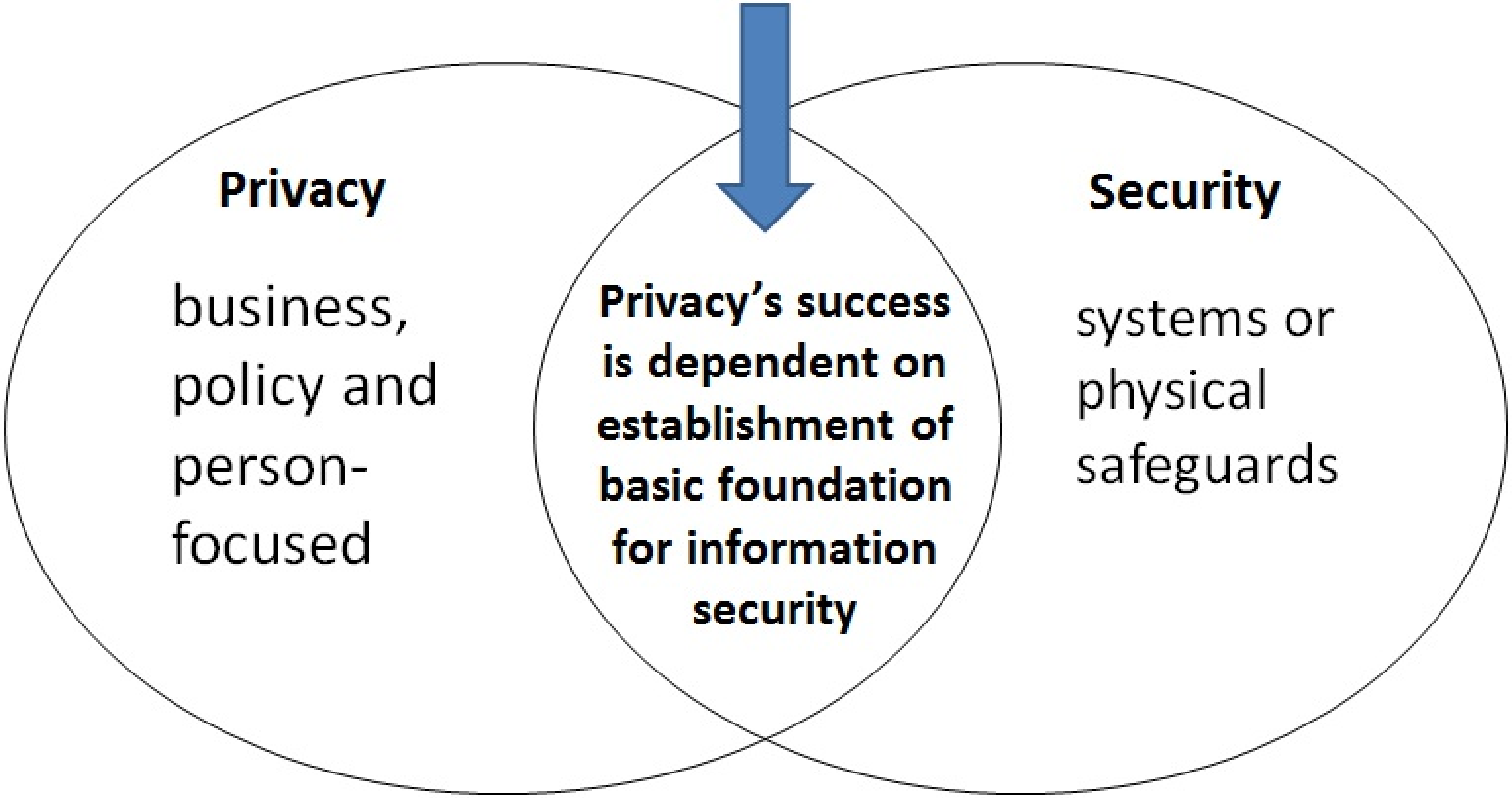
Agenda

1. Background on assister privacy and security requirements and highlights
2. NEW Guidance: How to obtain a consumer's authorization before gaining access to PII
3. NEW Guidance: CAC and Navigator model authorization forms
4. NEW Guidance: Best practices for handling PII: Fast Facts for Assisters
5. What additional resources are available?

1. Background on Assister Privacy and Security Requirements

- All Marketplaces, including the Federally Facilitated Marketplace (FFM), are required to have privacy and security standards (45 CFR 155.260(a)). **The FFM establishes assister privacy and security standards through agreements,** including:
  - Navigator grant terms and conditions
  - Agreement between CMS and CAC designated organizations
- Each Navigator and CAC organization in the FFM should refer to the privacy and security terms of its agreement, including the following provisions:
  - **Navigators:** Attachments E and F of grant terms and conditions
  - **CACs:** Appendix A of Agreement between CMS and CAC designated organization
  - **Both:** 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.

What's the difference between privacy and security?



Privacy

business, policy and person-focused

Privacy's success is dependent on establishment of basic foundation for information security

Security

systems or physical safeguards

CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF INFORMATION SERVICES

What is information security?

- The practice of **protecting information** from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
- **Procedures & controls** - the **“how to”** keep data confidential and safeguard systems
- **Minimum Acceptable Risk Standards for Exchanges (MARS-E)** primarily addresses security guidelines that apply to Navigators and CACs

What is “PII?”

- **Personally Identifiable Information (PII**) is any information that:
  - can be used to distinguish or trace an individual’s **identity**,
  - alone or when **combined** with other personal or identifying information
  - that is **linked** or **linkable** to that individual

OMB Memorandum M-07-16

Examples: citizenship or immigration status, applicant ID, household income, qualified health plan (QHP) eligibility status, language preference

Highlights of Navigator and CAC Privacy and Security Requirements in the FFM

- Navigators and CACs in the FFM are permitted to create, collect, disclose, access, maintain, store and use consumer PII to the extent necessary to perform required assister duties.
- The FFM Navigator and CAC privacy and security requirements address how these assisters should handle PII when performing their required duties.
- These privacy and security requirements are designed to ensure that:
  - consumers' information is accurate and current;
  - information is used only as is necessary and relevant to activity at hand;
  - all uses of information are known and consented to by consumer;
  - appropriate, swift action is taken when an incident or breach occurs; and
  - confidentiality is protected, to enable trust between the assister and the consumer.

2. NEW Guidance: How to Obtain a Consumer’s Authorization Before Gaining Access to PII

- CMS will release a new tip sheet that addresses how assisters may meet the consumer authorization requirement (45 CFR 155.210(e)(6), 155.215(g), and 155.225(f))
- Highlighted Content:
  - General overview of ways to obtain consumer authorization
  - Required and recommended content for authorization and record of authorization
  - Scenarios for obtaining consumer authorization
  - Ways to maintain a record of consumer authorization
  - Summary of updates to Navigator and CAC model forms
  - FAQs

3. NEW Guidance: CAC and Navigator Model Authorization Forms

- Restructured the forms into 4 main parts:

1. **Acknowledgment** that consumer received information about assister's roles and responsibilities, consistent with 45 CFR 155.210(e)(6)(i) and 45 CFR 155.225(f)(1). A list of roles and responsibilities is contained in "Attachment A."
2. **Definitions of terms**
3. **Authorizations:**
   - General consent
   - Specific consent(s)
   - Exceptions or limitations to consent
   - Additional information about the use of consumer PII
4. **Signature and contact information** for follow-up

3. NEW Guidance: CAC and Navigator Model Authorization Forms, *cont'd*

- Unless the consumer limits his or her consent to apply only to specific individual assisters, it is <u>not</u> necessary for a consumer to provide a separate authorization for each individual assister who helps that consumer. This means that a single authorization may extend to all the assisters within the same assister organization.
  - On the model authorization forms, each time "[Name]" appears on the forms, the name of the organization, at a minimum, should be inserted. Individual assister names may, but are not required to be inserted.
- To clarify that a consumer's consent applies to annual redetermination and re-enrollment processes, the **specific consent** section includes this activity.

3. NEW Guidance: CAC and Navigator Model Authorization Forms, *cont'd*

- Highlights under the **additional information** section:
  - Assister will only ask consumer for the minimum amount of PII necessary to help.
  - Assister will ensure that PII is kept private and secure when handling consumer's PII and will follow privacy and security standards in doing so.
  - Assister may follow-up after first meeting with consumer if consumer provides his or her contact information.
  - Assister might share consumer's PII when referring consumer to another source of help.
  - Assister will provide consumer with copy of assister's roles and responsibilities in Attachment A.
  - Space provided to tell consumers about any state requirements that require disclosure of consumer PII to a state authority.

4. NEW Guidance: Best Practices for Handling PII: Fast Facts for Assisters

- Highlights:
  - **Best practices** include:
    - Routine internal discussions about how your organization should protect consumer PII and ongoing monitoring of how well your organization protects PII, which could include taking additional training, beyond the annual Marketplace training.
    - When obtaining consumer authorization, develop and follow standard operating procedures and checklists.
    - When providing application and enrollment assistance:
      - Use private spaces, do not leave documents containing PII unattended, keep notes private and secure, and don't forward PII to personal email accounts.
  - Reminders regarding **breach and incident reporting for Navigators and CACs** as required by their privacy and security requirements.
  - **Consumer scenarios** illustrating best practices.

5. What additional resources are available?

- All new guidance will be posted on Marketplace.CMS.gov
  - Spanish versions of Navigator and CAC model forms will also be posted when available.
- As always, If you have questions about privacy and security requirements, you should direct your questions to:
  - Certified Application Counselors and Non-Navigator Assistance Personnel: CACQuestions@cms.hhs.gov
  - Navigators: NavigatorGrants@cms.hhs.gov
  - CMS contractors: contact appropriate CMS personnel
- **Reporting incidents or breaches**: Contact **CMS IT Service Desk** (available 24 hours a day, 7 days a week) immediately after discovery via:

  Phone: **410-786-2580** or **1-800-562-1963**

  Email: CMS_IT_Service_Desk@cms.hhs.gov