

PY27 Cert Training Module 9

Table of Contents

1. Title Slide	3
1.1 Title Slide	3
2. Your Personally Identifiable Information (PII) Responsibilities	4
2.1 Your Personally Identifiable Information (PII) Responsibilities	4
2.2 How PII is Used	4
2.3 What PII is Used.....	5
2.4 Safeguarding PII	5
2.5 Your Use of Customers' PII.....	6
2.6 Your Use of Customers' PII.....	6
2.7 Consequences of Not Protecting PII	7
3. Customer Consent	7
3.1 Customer Consent	7
3.2 Customer Consent	8
3.3 Record of Consent	8
3.4 Record of Consent	9
3.5 Record of Consent Retention Period	9
3.6 Photo/Image Consent Form	10
3.7 Privacy Notice Statement	10
3.8 Privacy Notice Statement	11
4. Reporting Privacy & Security Incidents.....	11
4.1 Reporting Privacy & Security Incidents.....	11
4.2 Privacy & Security Incidents	12
4.3 What is a Breach?	12
5. Reducing Threats & Risks.....	13
5.1 Reducing Threats & Risks.....	13
5.2 Threats to Your Computer	13

5.3 Malware.....	14
5.4 Security Controls	14
5.5 Password Protection.....	15
6. Final Slide	15
6.1 Final Slide	15

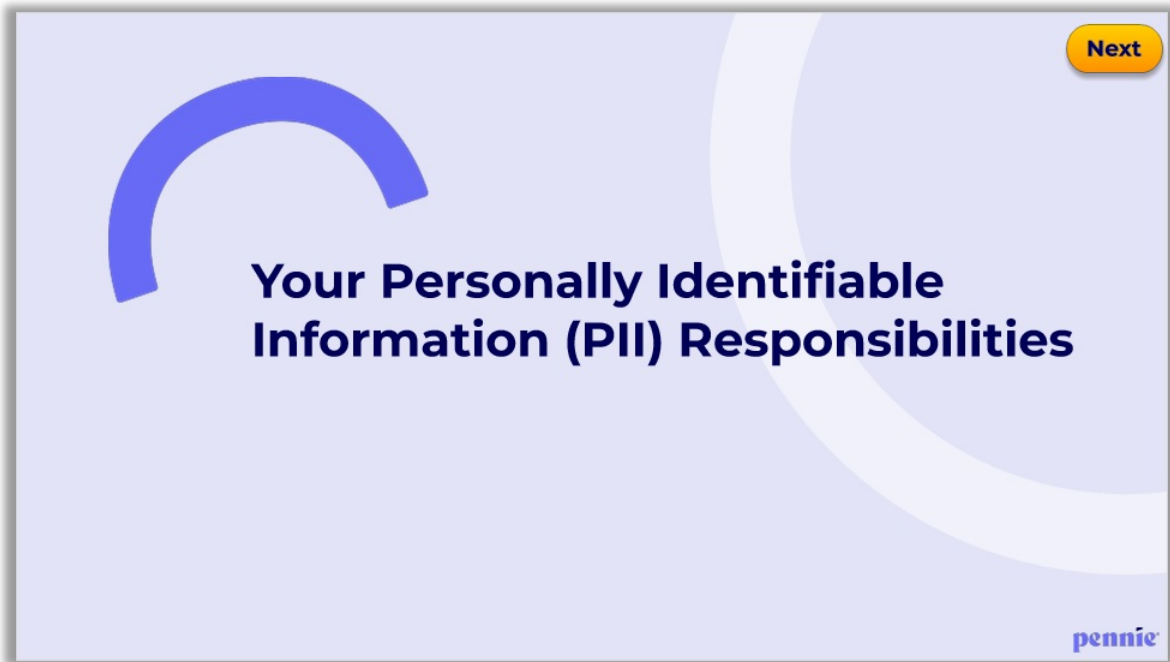
1. Title Slide

1.1 Title Slide



2. Your Personally Identifiable Information (PII) Responsibilities

2.1 Your Personally Identifiable Information (PII) Responsibilities



2.2 How PII is Used

How PII is Used

Customers should understand how their PII is used and for what reason.

Pennie enrollees can review the Pennie Privacy Policy posted at [Privacy | Pennie.com](#). In addition, the application filer must read and acknowledge Pennie's Privacy Policy when they start an application.

Pennie must collect information to authenticate identity, citizenship status, residency, income, and incarceration status in order to:

- Determine or assess eligibility for Pennie, MA, or CHIP coverage
- Determine or assess eligibility for financial savings
- Display QHP/QDP options
- Facilitate enrollment
- If applicable, process eligibility appeals

Assure customers that PII collected by Pennie will be used only for fulfilling the SBE functions.

Back Next

pennie

2.3 What PII is Used

What PII is Used

BackNext

The PII data collected for use in Pennie includes, but is not limited to:

- Identifying/Demographic Data
 - i.e., name, address, telephone number, email, age
- Income Data
 - i.e., tax filing status, marriage status, tax dependents, employer, annual or monthly income
- Citizenship and Immigration Data
 - i.e., SSN, Resident Alien Number, Native American Tribe ID Number, incarceration status
- Disability Information
 - i.e., whether the applicant/household member is blind, disabled, or requires assistance with daily living
- Medical Insurance Information
 - i.e., past and current health insurance, tobacco use, customer plan selections, and other information necessary to facilitate enrollment

pennie

2.4 Safeguarding PII

Safeguarding PII

BackNext

Assisters and brokers are responsible for protecting a customer's PII, and therefore are required to:

- Implement administrative, physical, and technical safeguards to protect PII from loss, theft, or inadvertent disclosure
- Ensure PII is only used by – or disclosed to – those authorized to receive or view it
- Protect against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of customer PII
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by Federal and State Law
- Securely destroy – or dispose of – PII in an appropriate and reasonable manner and in accordance with applicable retention schedules

pennie

2.5 Your Use of Customers' PII

Your Use of Customers' PII

BackNext

The following are some important restrictions on using a customer's PII. **You cannot:**

- Request or require an SSN or information regarding citizenship, status as a national, or immigration status for any customers *not* seeking coverage for themselves on any application, unless the customer has separately provided written informed consent for you to access this information
- Request information from – or concerning – any individual who is not seeking coverage for themselves, unless the information is needed for Pennie to determine an applicant's eligibility
- Collect PII beyond what is necessary to perform your authorized functions without the specific, informed consent of the customer

pennie

2.6 Your Use of Customers' PII

Your Use of Customers' PII

BackNext

In addition, **you cannot:**

- Directly or indirectly receive remuneration in exchange for any PII of an individual
- Use PII to discriminate against customers, such as refusing to assist individuals who are older or who have complex healthcare needs
- Make cold calls, send unsolicited emails, or use other means of unsolicited direct contact for the purpose of providing application or enrollment assistance, unless:
 - You have a pre-existing relationship with a customer
 - You have complied with all other applicable state and federal laws

pennie

2.7 Consequences of Not Protecting PII

Consequences of Not Protecting PIIBackNext

There are serious personal consequences associated with not protecting PII appropriately and/or purposefully disclosing PII for an unauthorized purpose. These include, but are not limited to:

- Civil penalties, including a Civil Money Penalty, up to \$25,000 per violation by the Federal Government
- Disciplinary action by the Pennsylvania Insurance Department (PID) and/or other agencies

In addition, failure to protect or disclose PII appropriately may cause:

- Harm to customers, including theft of their identity
- Loss of customer trust
- Disciplinary action by your organization
- Revocation of your Pennie certification



pennie

3. Customer Consent

3.1 Customer Consent

**Customer Consent**BackNext

pennie

3.2 Customer Consent

Customer Consent

[Back](#)[Next](#)

Before you assist customers, **you must discuss your role and responsibilities with them, and obtain consent to access their PII.** This is sometimes called getting the customer's "**authorization.**"

Customers may give consent themselves, or choose to have a legal or authorized representative provide consent on their behalf.

- A legal or authorized representative must have authority to act on a customer's behalf

You may obtain a customer's general consent to access their PII to carry out your authorized functions **only if a record of the consent is maintained consistent with Pennie requirements.**

To use PII for purposes unrelated to your authorized functions, you must obtain the customer's informed consent in writing.

The consent form should be written in plain language and must include the specific elements set forth in the privacy and security standards that apply to you and your organization.

Consent forms and materials should be made available in the languages spoken within the community.



3.3 Record of Consent

Record of Consent

[Back](#)[Next](#)

The **Record of a Customer's Consent** is one of the most important documents you will use in your work with a customer. Your organization may adapt the CMS model consent form, or develop your own form or procedures related to obtaining a customer's consent, as long as it includes, at a *minimum*:

- An acknowledgment that you informed the customer of your functions and responsibilities
- Consent for you to access and use the customer's PII to carry out your Pennie functions and responsibilities
- The **retention period**; you must specify that your organization is required to appropriately secure and retain a customer's PII for **ten years**
- The **expiration of consent**; under CMS regulations, assisters and brokers must permit customers to revoke their consent at any time during the retention period, which includes permitting customers to place a time restriction on the consent



3.4 Record of Consent

Record of Consent

[Back](#)[Next](#)

At a *minimum*, the record of the customer's consent should include:

- The customer's name and (if applicable) the name of the legal or authorized representative providing consent on the customer's behalf
- The date the consent was given
- Your name, or the name of the delegate to whom consent was given
- Notes regarding any limitations placed by the customer on the scope of the consent
- Notes recording all acknowledgments and consents obtained from the customer, including any applicable specific consent to access customer PII for state-approved purposes not included in the list of purposes set forth in your agreement with the Commonwealth
- If any changes are later made to the consent, including if a customer revokes the consent or any part thereof, these should be included with the original record

pennie

3.5 Record of Consent Retention Period

Record of Consent Retention Period

[Back](#)[Next](#)

For Pennie, the *minimum* amount of time your organization needs to keep a record of customers' consent is **10 years**, unless a different and longer retention period has been provided under other applicable federal law.

Customers may choose to grant consent indefinitely, or until unless they revoke their consent. Your organization can also choose to set its own expiration date for customer consent.

Under Pennsylvania regulations, assisters and brokers must permit customers to revoke their consent at any time, which includes permitting customers to place a time restriction on the consent at any time.



pennie

3.6 Photo/Image Consent Form

Photo/Image Consent Form

BackNext

During an enrollment assistance event or meeting, you may take photos or videos of customers and wish to use those photos or videos for promotional activities, or to share them with Pennie to use for marketing and outreach materials. Before you share or use the photos or videos, you should obtain the customer's consent for use.

A [Pennie Consent to Use of Picture and/or Voice Form](#) is available on Pennie.com and should be used and retained for this purpose.

This form may be modified to include your organization as long as Pennie remains on the form to be released. You may *not* use your organization's release form and add Pennie without permission.

Your organization is to store the form in accordance with your organizational policies for document retention.

pennie

3.7 Privacy Notice Statement

Privacy Notice Statement

BackNext

In addition to the Customer Consent Form, before you can collect PII or other information from customers, you and/or your organization must provide a them with a **Privacy Notice Statement**. The statement explains:

- What personal information is collected
- Why it's collected
- How it will be used
- With whom the information can be shared
- For what purposes it can be shared
- How the information will be kept secure

Pennie customers can review the Pennie Privacy Policy posted at [Privacy | Pennie.com](#). In addition, an application filer must read and acknowledge Pennie's Privacy Policy when they start an application.



pennie

3.8 Privacy Notice Statement

Privacy Notice StatementBackNext

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 with disabilities and/or Limited English Proficiency.

If your organization maintains a website that is used to gather or request PII or other customer information, the Privacy Notice Statement must be prominently and clearly displayed on the organization's website.

The Privacy Notice Statement should explain how customers can file a complaint with Pennie and your organization – related to you and/or your organization's activities – with respect to their information.

Your organization must review the Privacy Notice Statement at least annually and revise as necessary, including after any change to the organization's privacy policies and procedures.

Note: You are permitted to collect a customer's name, mailing address, email address, or telephone number without first providing a written Privacy Notice Statement if you are using this information solely to:

- Follow up with the customer to conduct an authorized function, such as scheduling an appointment for application assistance
- Send the customer educational information that is directly relevant to your authorized functions

pennie

4. Reporting Privacy & Security Incidents

4.1 Reporting Privacy & Security Incidents

**Reporting Privacy & Security Incidents**BackNext

pennie

4.2 Privacy & Security Incidents

Privacy & Security Incidents

[Back](#)[Next](#)

Privacy and security incidents are potential threats to the confidentiality, integrity, or availability of PII.

A **security incident** is the act (or attempt) of violating an explicit or implied security policy, which includes attempted or successful unauthorized access, use, disclosure, modification, or destruction of data, or interference with system operations in an information system.

A **privacy incident** is a security incident where individuals other than authorized users have access to PII.

Examples of privacy incidents include:

- Losing electronic devices that contain PII
- Losing documents containing PII
- Sharing paper or electronic documents containing PII with individuals unauthorized to access it
- Accessing documents containing PII without authorization
- Posting PII to a public-facing website
- Mailing hard copy documents containing PII to the incorrect address
- Leaving documents containing PII exposed in an area where individuals without approved access could access them

pennie

4.3 What is a Breach?

What is a Breach?

[Back](#)[Next](#)

A **Breach** is a privacy incident that poses a risk of harm to applicable individuals. A breach occurs when:

- A person other than an authorized user accesses or potentially accesses PII
- An authorized user accesses or potentially accesses PII for a non-authorized purpose

If you learn of any situation in which a customer's PII has been compromised in any way, including loss of records or devices, or unauthorized persons seeing or possessing the information, the incident must be reported to Pennie at privacy@Pennie.com within 24 hours of discovery (to align with CMS guidelines).

The determination of whether a privacy incident rises to the level of a breach **is made by Pennie**.

Because your organization is approved to provide assistance to customers, **it must have written procedures for addressing privacy and security incidents, including breaches**. These procedures for reporting must address how to identify incidents, and identify the organization's designated personnel (e.g., a Privacy Officer) responsible for reporting and managing incidents or breaches to Pennie.

pennie

5. Reducing Threats & Risks

5.1 Reducing Threats & Risks



5.2 Threats to Your Computer

Threats to Your Computer Back Next

It's essential that any computers you use are protected from harmful computer programs, applications, and **malware (malicious software)**.

It is your responsibility to make sure that computers in your office used to access Pennie are regularly updated with Operating System updates and the latest security software to protect against any cyber-related security threats.

In addition, **never join or utilize an unsecured or public Wi-Fi network, especially to access Pennie.** Unsecured and public Wi-Fi networks have little or no security to protect against bad actors who may use the network to steal information.

pennie

5.3 Malware

Malware

[Back](#)[Next](#)

Malware is software designed to harm or secretly access a computer system without the owner's consent. It's a generic term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Malware is consistently sent by email. These messages are disguised as regular messages from trusted sources.

Always check the sent from URL to identify suspicious messages. If the sender's URL seems peculiar, do *not* click on any links or attachments contained in the message. You should then notify your organization's network security contact.

Corrupted websites may deliver malware through fake links, ads, or pictures. Public computers, such as those accessed in a library, may be particularly susceptible to malware and viruses. If you have to assist a customer using public computer, never save private files or passwords to the computer.



pennie

5.4 Security Controls

Security Controls

[Back](#)[Next](#)

You can apply certain **Security Controls** to protect information. **Security controls** are policies, procedures, and practices designed to manage risk and protect IT assets.

Common examples of controls include:

- Security awareness and training programs
- Physical security like guards, badges, and fences
- Restricting access to systems that contain sensitive information
- Changing your password often and immediately if you suspect it has been compromised

Your organization is required to monitor, periodically assess, and update its security controls and related system risks to maintain continued effectiveness of those controls.

pennie

5.5 Password Protection

Password Protection Back Next

Some examples of steps you can take to help promote security on information systems that store customer PII include:

- Changing your password often
- Changing your password immediately if you suspect it has been compromised
- Using a different password for each system or application
- Using a secure, encrypted password manager
- Choosing a password that is not generic and easily obtained, such as family member names, pet names, birth dates, phone numbers, or vehicle information
- Never share your password with anyone
- Never leave your password in an unsecured space, such as written down beside your computer, where others could see it

pennie

6. Final Slide

6.1 Final Slide

Back Exit

pennie

ADDRESS	PHONE	WEB
P.O. Box 11873	+1 844-844-8040	Pennie.com
Harrisburg, PA 17108-1873		