Georgia Access Certification Training for Plan Year 2025

Privacy & Security for Navigators/ CACs Training Manual

July 31, 2024

h

Table of Contents

1 Module Introduction

1.1 Module Objectives

a. Determine what is and what is not Personally Identifiable Information (PII) and Protected Health Information (PHI).
b. Understand the rules and regulations pertaining to privacy and security for Georgia Access.
c. Understand your role in handling and safeguarding PII and PHI information.

2 Introduction

2.1 Privacy & Security Standards

a. Georgia Access is focused on ensuring that all consumer data is safeguarded pursuant to federal and state laws.

2.2 Definition of Privacy & Security

a. *What is privacy?* Privacy is the individual right for a consumer to manage how their personal information is viewed and accessed.
b. *What is security?* Security refers to the protection against unauthorized access to a consumer's personal information.

2.3 Sensitive Information

a. In performing your duties, you will have access to sensitive client information or Personally Identifiable Information (PII) that may include Protected Health Information (PHI). Rules and regulations were established through the Health Insurance Portability and Accountability Act (HIPAA) to enforce the protection of PHI. When assisting consumers, you should collect the minimum information needed to determine consumer eligibility for Qualified Health Plans (QHPs) and subsidies. You should access PHI only if absolutely necessary (e.g., if that information is needed to help a consumer qualify for a Special Enrollment period (SEP)).

2.4 Penalties & Violations

a. Failure to handle PII carefully may violate privacy and security laws, which could result in civil and criminal penalties. This training is designed to assist you in protecting consumer data and avoiding violations.

2.5 Knowledge Check

a. When should you collect Protected Health Information (PHI)?
   i. Never
   ii. Only when necessary
   iii. Always

3 Legislation, Rules, & Regulations

3.1 Affordable Care Act (ACA) Personally Identifiable Information (PII) Regulations

a. The ACA and associated federal regulation 45 CFR 155.260 describes how agents, Navigators, and Certified Application Counselors (CACs) are required to handle consumer PII. These rules aim to

protect privacy and secure consumer PII within the operations of a State-based Exchange (SBE) and apply to all non-Exchange entities.

b. A non-Exchange entity is any individual that gains access to PII submitted to an Exchange, collects, uses, or discloses PII gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange. Certified agents, Navigators, CACs, and agency administrative staff are all considered non-Exchange entities and must adhere to the regulations in 45 CFR 155.260.

3.2 HIPPA Overview

a. Established in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a key federal law that governs the collection and use of consumer health data. It was established to:
   i. Make it easier for consumers to keep health insurance
   ii. Protect the confidentiality of consumer healthcare information
   iii. Ensure that consumer healthcare data is secured properly
   iv. Help the healthcare industry control administrative costs
   v. Ensure that consumers have access to health records
   vi. Create national standards for the safeguarding of PHI
   vii. Promote administrative simplification

b. Key HIPAA Rules & Regulations
   i. There are five federal rules that support HIPAA legislation. For this training, the four rules applicable to assisting consumers will be covered. These have an effect on day-to-day work activities and could result in penalties if not followed.
      1. *Rule 1: HIPAA Privacy Rule*. The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of Protected Health Information (PHI) and sets limits and conditions on the disclosure, maintenance, and use of such information without an individual's prior authorization. These national standards were established to protect consumers' medical records and other PHI.
      2. *Rule 2: HIPAA Security Rule*. The HIPAA Security Rule establishes national standards to safeguard consumers' electronic PHI that is created, received, used, maintained, or transferred by a covered entity.
      3. *Rule 3: HIPAA Enforcement Rule*. The HIPAA Enforcement Rule relates to compliance and investigations, the imposition of civil penalties for violating the HIPAA Administrative Simplification Rules and sets hearing procedures when violations have been committed and reported.
      4. *Rule 4: HIPAA Breach Notification Rule*. The HIPAA Breach Notification Rule requires HIPAA-covered entities and their business associates to provide notification following an incident of unsecured PHI to affected parties, government agencies, and possibly the media. A breach's severity can be determined by the following factors:
         i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
         ii. The unauthorized person who used the PHI or to whom the disclosure was made.
         iii. Whether the PHI was actually acquired or viewed.
         iv. The extent to which the risk to the PHI has been mitigated.
         v. The size and nature of the breach.

3.3 HIPAA Covered Entities

a. HIPAA applies to covered entities including healthcare providers, health plans, or healthcare clearinghouses that electronically transmit any health information.
b. PHI is defined as Individually Identifiable Health Information (IIHI) transmitted or maintained by a covered entity or its business associates in any form or medium. HIPAA requires those who handle confidential data to effectively safeguard the data.
c. Business associates of covered entities includes:
    i. Contractors, subcontractors, or other outside persons/companies that are not employees of a covered entity will need access to health information when providing services to the covered entity.
    ii. Generally, certified agents, agency administrative staff, Navigators, and CACs are considered business associates of covered entities.
    iii. Covered entities must have contracts that include HIPPA reporting requirement terms in place with their business associates.
d. Since HIPAA establishes standards for securing healthcare information, it's important to understand what types of entities are covered.
    i. Who is generally considered a covered entity under HIPAA?
        1. Health Insurance Companies
        2. Health Maintenance Organizations (HMOs)
        3. Company Health Plans
        4. Government programs that pay for healthcare
    ii. Which type of healthcare providers are typically covered entities?
        1. Doctors
        2. Clinics
        3. Psychologists
        4. Dentists
        5. Chiropractors
        6. Nursing Homes
        7. Pharmacies
e. Healthcare clearinghouses are also covered entities. They are entities that process nonstandard health information they receive from another entity into a standard, or vice versa.

3.4 Information Protected by HIPPA

a. Consumer information in an insurance company’s computer system
b. Any information that doctors, nurses, and other health care providers put in a consumer’s medical record
c. Conversations a doctor has about a consumer’s care or treatment with nurses and others
d. Billing information
e. Other consumer health information held by those who must adhere to HIPAA

3.5 Georgia Access Policy

a. Georgia Access has a privacy policy, linked here: https://georgiaaccess.gov/privacy-policy/. All certified agents, agency administrative staff, Navigators, and CACs are expected to be familiar with this policy.

3.6 Knowledge Check

a. All of the following are goals of HIPAA except:

i. Make it easier for consumers to keep health insurance.
ii. Protect the confidentiality of consumer healthcare information.
iii. Ensure that consumer healthcare data is secured properly.
iv. Lower the cost of monthly premiums.

4 Types of Protected Information

4.1 Personally Identifiable Information (PII)

a. PII is information that can be used to distinguish or trace a consumer's identity when it's accessed alone, or when combined with other personal or identifying information that can be linked to a specific consumer. The majority of consumer information in the Georgia Access system is PII (not PHI). Consumer information collected to determine eligibility for Qualified Health Plans (QHPs), Stand-alone Dental Plans (SADPs), and financial subsidies is considered PII. Information collected for tax purposes and tax credits is also PII. Per 26 U.S. Code § 6103, tax returns and return information are confidential.

4.2 What does PII look like?

a. Listed below are common forms of PII:
   i. Name
   ii. Date/Place of Birth
   iii. Phone Number
   iv. Address
   v. Mother's Maiden Name
   vi. Social Security Number
   vii. Email Address
   viii. Employment Information
   ix. Biometric Information

4.3 Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI)

a. Individually Identifiable Health Information (IIHI) is health information created or received by a healthcare provider, health plan, employer, or healthcare entity that relates to the condition of a patient. Not all IIHI is PHI. IIHI becomes PHI (according to 45 CFR §160.103) when it is transmitted or maintained in any form or medium. You may gain access to PII submitted to an Exchange. PHI should be collected only when absolutely necessary due to privacy concerns. In some cases, PII, IIHI and PHI identifiers may overlap.

4.4 PHI Identifiers

a. The following are 17 common PHI identifiers:
   i. Names
   ii. All dates related to the health or identity of the individual
   iii. Geographic locators
   iv. Phone numbers
   v. Fax numbers
   vi. Email addresses
   vii. Social Security Numbers
   viii. Medical record numbers
   ix. Health plan beneficiary numbers
   x. Certificate license numbers

xi. Account numbers
xii. Vehicle identifiers
xiii. Device identifiers
xiv. Web URLs
xv. IP addresses
xvi. Biometric information
xvii. Full face photograph

4.5 Knowledge Check

a. True or False: PII contains demographic information and personal information that may be able to identify a consumer, while PHI is specifically health-related information.
   i. True
   ii. False

5 Protecting PII & PHI

5.1 Handling PII & PHI

a. While helping consumers understand their health insurance coverage options on Georgia Access and assisting them with the application, you will be exposed to sensitive client information that is considered Personally Identifiable Information (PII) and have a high likelihood of also being exposed to Protected Health Information (PHI). You must handle PII and PHI carefully and should not leave them in public places or areas where others may be able to access them. It's a legal requirement to always follow the privacy and security rules of handling consumers' personal information. Failure to do so will result in penalties, which we will cover later in this module.

5.2 PII & PHI Handling Requirements

a. Consumer Authorization
   i. Before gaining access to a consumer's PII, Navigators and CACs must obtain the consumer's written authorization. The steps below describe how you will do this.
      1. *Clarify your role & responsibilities.* One of the first steps you must take when providing application assistance is informing the consumer about your roles and responsibilities and obtaining the consumer's authorization to access their PII (sometimes referred to as obtaining consumer's consent). In addition, you are required to distribute a Privacy Notice to the consumer. A Privacy Notice provides a clear, user-friendly explanation of the consumer's rights with respect to PII and PHI and the privacy practices of your interactions.
      2. *Obtain written authorization to access PII & PHI*. Make sure the consumer provides you with authorization to access their PII or PHI by completing and signing a written form before sharing their PII or PHI, and let the consumer know they can revoke that authorization at any time.
      3. *Maintain records*. You must retain records of PII and PHI authorization for 6 years, in accordance with federal regulations.

5.3 Maintaining a Record of Authorization

a. Keeping a record of a consumer's authorization should include an authorization form. At a minimum, the record of authorization should include the following:
   i. The consumer's name and (if applicable) the name of the consumer's legal, authorized representative.

ii. The date the authorization was given.
iii. Your name, or the name of the person who was provided authorization.
iv. Any limitations placed by the consumer on the overall scope of authorization.
v. Any notes recording all acknowledgments and consents agreed to by the consumer.
vi. If any changes are made to the authorization at a later point in time, including if and when a consumer revoked the authorization.

b. The Authorization Form for Georgia Access will be provided to Navigators and CACs prior to Open Enrollment.

5.4 PII Authorization Scenarios

a. Scenario 1: Over the Phone/Computer
   i. *Scenario*: You are assisting the consumer remotely over the phone or computer and need to obtain their authorization.
   ii. *Obtaining authorization*: You can gain a consumer's authorization by reading the authorization form. After the authorization form is read, record in writing that the consumer's authorization was obtained. Finally, create a record of the authorization as it is being provided, and then read back the content of the record to the consumer once it is complete so that the consumer can confirm that the record is accurate and complete.
b. Scenario 2: A Sign-Up Sheet at an Outreach Event
   i. *Scenario*: A sign-up sheet is used to collect a consumer's information at an outreach event.
   ii. *Obtaining authorization*: It must be stated on the sign-up sheet that by providing their information, they are consenting to being contacted and that this information must be securely stored and only accessible by those who need it for required tasks.
c. Scenario 3: Consumer Volunteers Information
   i. *Scenario*: You may receive a direct phone call, voicemail, or email from a consumer requesting your services and volunteering information containing PII to you. You are required to obtain a completed authorization form when you follow up with the consumer.
   ii. *Obtaining authorization*: If a consumer directly contacts you or your organization for assistance and shares their PII, you should still obtain a complete authorization from the consumer the next time you follow up with them. Any PII collected in the initial contact should still follow the requirements for maintaining authorization records.
d. Scenario 4: A Third-Party Initiates Contact and Volunteers a Consumer's PII
   i. *Scenario*: You may encounter a situation where a third party shares a consumer's PII with you without the consumer being present. This may raise concerns that the consumer had not authorized the third party to share their PII with you.
   ii. *Obtaining authorization*: Consumer PII obtained via a third-party (not directly from the consumer) must still follow consent requirements to maintain authorization records. You will be required to obtain a completed consent authorization form from the consumer once you follow up with them.
e. Regardless of the scenario, it is imperative that you always obtain a signed copy of the authorization form.

5.5 General Protection

a. You must handle PII and PHI carefully and should not leave it in public places or areas where others may be able to access it. PII and PHI must be kept secure and safeguarded from being accessed by unauthorized personnel.
b. PII and PHI handling requirements:

i. All information received must be kept confidential in accordance with applicable state and federal laws and regulations.
ii. Only information required to assist the consumer can be gathered/collected.
iii. Share consumer PII and PHI only with those who are authorized to receive such information.
iv. Establish guidelines and safeguards to prevent the unauthorized release of individual consumer information to the public.
v. Maintain compliance with the policies and processes established by your organization for handling PII and PHI on Georgia Access.
vi. Report all privacy and security incidents for Georgia Access consumers, including misuse or loss of consumer PII, immediately.
vii. When meeting with consumers either virtually or in-person, ensure that the location is appropriately private to avoid others being able to access PII or PHI; do not leave any materials in plain sight.
viii. It's a legal requirement to always follow the privacy and security rules of handling consumers' personal information.
ix. Failure to adequately protect the security of PII and PHI may result in civil and criminal penalties levied against you and your organization.

5.6 Protecting PII & PHI

a. PII and PHI must be kept secure and safeguarded from being accessed by unauthorized personnel. If PII and PHI are not properly safeguarded, consumers' identities and information may be exposed to individuals, both internally and externally, who are not permitted to receive such information. Failure to adequately protect the security of PII and PHI may result in civil and criminal penalties levied against you and your organization.

5.7 Protecting PII & PHI in the Office

a. Make sure consumers take possession of their documents.
b. Secure hard-copy consumer consent forms in a locked location.
c. Restrict access so only authorized individuals have access to PII and PHI and/or are allowed in areas where PII and PHI may be accessed.
d. Maintain employee awareness and train employees on how to safeguard PII and PHI.
e. Ensure that consumers' scanning and copying equipment doesn't electronically retain copies of the images.
f. Dispose of PII and PHI in a manner consistent with Georgia Access rules and retention requirements.
g. If consumers leave documents containing PII and PHI with you by accident, you should store them in a safe, locked location and return them to them as soon as possible.
h. During consumer appointments, in-person, over the phone, or virtually, utilize private spaces to ensure confidentiality and privacy.
i. Never repeat PII and PHI in a situation where others can hear it.
j. PII and PHI collected from a consumer—including name, email address, telephone number, application ID number, addresses, or other notes—must be stored securely.

5.8 Protecting PII & PHI Electronically

a. Verify that "auto-fill" settings on your Internet browsers are turned off.
b. Maintain computer security, including the use of a secure wireless network, when performing assistance using an authorized mobile device (for example, a tablet).
c. Don't send or forward emails with PII to personal email accounts.

d. Protect emails that contain PII or PHI (for example, use encryption).
e. Don't upload PII and PHI to unauthorized websites (for example, wikis).
f. Don't use unauthorized mobile devices to access PII or PHI.
g. Lock up portable devices (for example, laptops or cell phones).
h. Clear web browser history to avoid other users accessing PII and PHI.
i. If in electronic format, PII and PHI should be stored securely in a password-protected file on a password-protected computer which only authorized individuals have access.

5.9 Protecting PII & PHI on Paper

a. Encourage consumers to verify mailing addresses before they send forms.
b. Don't leave files or documents containing PII and PHI (including tax return information) unsecured and unattended on desks, printers, fax machines, personal computers, phones, or other electronic devices.
c. Always make sure any originals of consumers' records are returned before they leave your facility, and only make copies for yourself or others if necessary to carry out required duties.
d. If in hard copy, PII and PHI must be stored securely, like in locked filing cabinets or in locked offices where the paper filing system is maintained.
e. It can be helpful to have a supply of manila folders to give to consumers with their documents inside to keep them in one place and shield the contents from view.

5.10 Knowledge Check

a. True or False? Jorge (a Navigator) noticed that Emma (another Navigator) isn't securely storing documents when she leaves for the day and instead, leaves them out on her desk for people to see as they walk past. These documents reveal some client PII and PHI. Emma is not effectively protecting PII and PHI.
   i. True
   ii. False

6 Security Incidents

6.1 What is a Security Incident?

a. A security incident is the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that has resulted in or is likely to result in the misuse of personal information. There are many types of security incidents, most notably, a breach.
b. A breach is the acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted and that compromises the security or privacy of the PHI. While a breach is a type of security incident, not all security incidents are/or result in breaches. It is important to note that security incidents and breaches are handled differently.
c. It's best practice to clear your desk of confidential data, files, and papers at the end of the day.

6.2 Examples of Security Incidents

a. *Computer threats*. Computer threats like malware or unsecured networks may lead to data leakage or complete access of your computer's data and files by an unapproved third party.
b. *Breaches*. Breaches occur when unapproved third parties gain access to systems, accounts, or networks through failure to maintain safeguards or accidentally being granted access knowingly or unknowingly by internal members.

c. *Password protection*. Maintaining complex, unique passwords and regularly changing those passwords is crucial. It's also crucial to never share created passwords.
d. *Email security incidents*. Email security incidents such as phishing may appear as legitimate emails but can result in breaches if opened or if hyperlinks within the email are clicked. It's best to verify all details of emails before responding or clicking on links included in emails.

6.3 Reporting Security Incidents

a. According to HIPAA's Security Rule, it's crucial for those who suspect or who have witnessed a security incident to follow the required reporting procedures.
b. HIPAA Breach Notification Rule
    i. Requires covered entities to notify affected individuals, the Secretary of Health and Human Services, and in some cases, the media of a breach of unsecured PHI. The reporting of breaches is driven by the size (e.g., more than 500 employees or less than 500 employees), and the Business Associate Agreement (BAA).
    ii. The BAA may have additional requirements for reporting than those required by the Breach Notification Rule but may not otherwise override the Rule's requirements for notification of breaches of unsecured PHI. Ultimately, Georgia regulations will dictate what is included in the BAA.
c. Relevant Code Federal Regulations (CFRs)
    i. 45 CFR Part 155: These standards outline the privacy and security requirements for Exchanges under the ACA and is crucial for Navigators and Consumer Assistance Programs.
    ii. 45 CFR Part 160 and 164: These sections implement the administrative simplification provisions of HIPAA and include the Privacy, Security, and Breach Notification Rules.
d. For breaches involving unsecured PII, Navigators and CACs are required to report the incident immediately to Georgia Access, and no later than twenty-four (24) hours, after discovery of the incident.
e. It is also the responsibility of each Navigator and CAC to maintain compliance with privacy and security standards for handling PII and PHI set by the organization with which you are affiliated (your Navigator Grantee Organization or Certified Application Counselor Designated Organization (CDO)). You must report any privacy and security incidents, including misuse or loss of consumer PII, to your affiliated organization immediately.

6.4 How to Combat Risks

a. *Protecting computers*: Devices containing PII and PHI must be secured to ensure compliance.
    i. Password-protect all devices and applications that contain PII and PHI.
    ii. Ensure that computers have the automatic time-out enabled.
    iii. Clear internet cache frequently.
    iv. Lock computer when walking away from it.
    v. Connect only to secure networks.
b. *Establishing controls*: Data that contains PII and PHI stored on or accessible from physical devices must be equipped with access controls.
    i. Lock all devices with a password or key.
    ii. Set app controls to require a password or multi-factor authentication each time a user logs in.
    iii. Never access client data on public computers.
    iv. Establish controls managing who may access office computers.
    v. Never permit others to use devices that contain PII and PHI.

c. *Guarding passwords*: Passwords are one of the most essential tools for safeguarding sensitive data and maintaining them correctly offers additional security.
   i. Choose longer, more complex, and unique passwords that would not normally be used.
   ii. Never give out passwords.
   iii. Never write passwords down.
   iv. Never save a password in a browser or an app.

6.5 Knowledge Check

a. Data that contains PHI stored on or accessible from physical devices must be equipped with _____.
   i. Wi-Fi
   ii. Access controls
   iii. Accessibility
   iv. A camera

7 Violations & Penalties

7.1 Violations & Penalties

a. Failure to maintain compliance with privacy and security standards to protect consumers' PII and PHI on Georgia Access may result in violations and/or penalties.
   i. *Violations*: Failure to comply with HIPAA and/or state/federal regulations will result in a violation and potential legal action.
   ii. *Penalties*: Penalties are the result of violations. These penalties can be categorized as either civil or criminal depending on the nature of the violation.
b. Consequences for violating section 1411(g) of the Affordable Care Act (ACA) will be subject to a Civil Money Penalty (CMP) of not more than $25,000 as adjusted annually under 45 CFR part 102 per person or entity, per use or disclosure, consistent with the bases and process for imposing civil penalties specified at §155.285, in addition to other penalties that may be prescribed by law.

7.2 Civil Penalties

a. When violations result in monetary fines from the State of Georgia or the federal government, the fines associated with the violation are considered civil penalties.
b. These civil penalties are broken up by four (4) categories of severity/violation:
   i. *Tier 1: Lack of Knowledge*. This tier is incurred when a covered entity is unaware of and could not have realistically avoided the violation with reasonable diligence.
   ii. *Tier 2: Reasonable Cause*. This tier is incurred when a covered entity should have been aware of the violation by exercising reasonable diligence.
   iii. *Tier 3: Willful Neglect – Corrected*. This violation is incurred as a direct result of "willful neglect", however, the issue was identified and corrected within 30 days.
   iv. *Tier 4: Willful Neglect – Not Corrected within 30 Days*. This violation is incurred as a direct result of "willful neglect", in cases where no attempt has been made to correct the violation.

7.3 Criminal Penalties

a. Criminal penalties occur when violations result in the wrongful disclosure of Individually Identifiable Health Information (IIHI). Criminal penalties often include imprisonment and a fine.
b. These are broken up by three (3) categories of severity/violation:

i. *Tier 1: Wrongful disclosure of IIHI*. This penalty is incurred when covered entities knowingly obtain or disclose IIHI wrongfully. Repercussions include a fine of up to $50,000 and imprisonment for up to one (1) year.
ii. *Tier 2: Wrongful disclosure of IIHI committed under false pretenses*. This penalty is incurred when covered entities knowingly obtain or disclose IIHI under false pretenses. Repercussions include a fine of up to $100,000 and imprisonment for up to five (5) years.
iii. *Tier 3: Wrongful disclosure of IIHI committed under false pretenses with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm*. This penalty is incurred when covered entities knowingly obtain or disclose IIHI under false pretenses with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm. Repercussions include a fine of up to $250,000 and imprisonment for up to ten (10) years.

7.4 Knowledge Check

a. Covered entities who knowingly obtain or disclose IIHI under false pretenses with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm may be sentenced up to ____ years in prison.
   i. One (1)
   ii. Five (5)
   iii. Seven (7)
   iv. Ten (10)

8 Additional Resources

8.1 Additional Privacy and Security Information:

a. Georgia Access Website: For more information regarding Georgia Access and additional resources, visit the Georgia Access Website
b. Federal Regulations for Privacy and Security
   i. Regulations 155.260: For more information on the specific privacy and security regulations outlined by the federal government, visit the linked website.
   ii. Federal Information about HIPAA: To view the Federal Information about HIPAA, visit the linked website.