There is no sound through your computer. You must dial-in on the telephone in order to hear the sound.

Time: 10:00am – 11:30am
Date: Wednesday July 21st, 2021
Dial-In Number: 1-855-897-5763
Conference ID: 1927368
TODAY’S WEBINAR

If you see this message when logging into the webinar…

Please find this email:
Subject Line 2021 Recertification Overflow Webinar I Privacy & Security
and click on the second link in order to log in.

Dial-In Number: 1-855-897-5763
Conference ID: 1927368
There is no sound through your computer.

• Dial in to listen to the audio portion of the webinar using the audio instructions on your WebEx control panel.

• All participants will remain muted for the duration of the program.

Dial-In Number: 1-855-897-5763
Conference ID: 1927368
QUESTIONS

Questions can be submitted using the Q&A function on your WebEx control panel.

• Chat function is disabled, please use Q & A panel to submit questions.
• We will pause near the end to take questions.
A recording of the webinar and any related materials will be available online on our Spring Training webpage. Please visit: https://info.nystateofhealth.ny.gov/SpringTraining
Webinar Statistics:

• Over 98% of respondents said the webinar increased their knowledge of the topic!
• The same percentage of people, 98%, said information from the webinar will allow them to better assist consumers!

Here’s what you said:

• “This webinar was very helpful in understanding the changes. It was exciting to learn about things that will really help my clients.”
• “Can you provide more information on the nearly-free Silver plan for unemployment recipients?”
PRESENTERS

Welcome

Gabrielle Armenia  Director, Bureau of Child Health Plus and Marketplace Consumer Assistance

Speakers

Marwan Diallo  Technical Architect, NY State of Health
Kelly Lamendola  Director, Office of Marketplace Counsel
Norman Massry  Chief Information Security Officer, NY State of Health
Karilyn Tremblay  Health Program Administrator 2, Bureau of Child Health Plus and Marketplace Consumer Assistance
Marketplace Assistors are required by law, to protect Personally Identifiable Information (PII) and Protected Health Information (PHI).

This training will cover:

- Definition of PII
- HIPAA and the Definition of PHI
- Limits on the Use of PII and PHI
- Requirements for Safeguarding PII and PHI
- Review of Best Practices
WHAT IS PII?

PII is Personally Identifiable Information. PII is information that can be used to distinguish a person’s identity, when standing alone or when combined with other information. Some examples include:

• Name
• Address
• Telephone number
• SSN
• Date of Birth
• E-Mail address
• Driver’s license number
• Passport number
USE OF PII

• The Marketplace uses PII provided by applicants to process eligibility determinations for public health insurance programs and QHPs.

• The Marketplace is subject to specific privacy and security standards for the collection, use and disclosure of PII under the federal Marketplace regulations (45 CFR 155.260).

• PII may only be used for eligibility and enrollment purposes. It may not be re-disclosed or shared for other purposes.

• PII may not be shared with other government agencies, except as permitted by law.
The Marketplace privacy and security regulations require “Openness and Transparency” regarding policies, procedures and technologies that directly affect consumers and their personal information.

Assistors should answer consumers’ questions about the need for identity proofing to protect privacy; and the need to collect PII to determine eligibility for coverage.

In addition, it is important that consumers review the general privacy attestation and the Terms, Rights and Responsibilities.
ASSISTORS AND PII

• Assistors must not keep copies of consumer documents, such as copies of passports.
  o If the consumer can’t finish the appointment, he or she should take their documents with them until they can reschedule.
  o Alternatively, there are other ways for consumers to submit their own documents, such as the mobile app (more to come on this later).

• Documents containing PII may be provided to the Assistor in-person or by regular mail.
  o For example: if following an in-person appointment, a consumer needs to provide additional copies of paystubs, the consumer may hand deliver or mail the documents to the Assistor in a sealed envelope, clearly marked with the Assistor’s name and organization (including client name and AC number). Assistor organizations may provide self-addressed labels for this purpose.
Can consumers fax documents, such as their paystubs, to their assigned Assistor?

Yes, consumer documents containing PII may be faxed to an Assistor.

- A consumer may fax their documents to an Assistor.
  - The Assistor must verify that the consumer has the correct fax number.
  - The Assistor agency must ensure that the facsimile machine is in a secure location and that the recipient Assistor is able to promptly receive the faxed information.
  - The fax cover page should include the name of the Assistor as well as the consumer’s name and AC number.
ASSISTORS AND PII, CONTINUED

• Assistors may maintain the names and telephone numbers of clients to make individual appointments and follow-up (as needed) regarding Marketplace coverage.

• Other client information must be stored in the Assistor dashboard.

• Contact information for clients must not be used for any other program purpose. Its use is limited to Marketplace enrollment assistance.
Faxing Identity Proofing Documents to the Marketplace

• Any fax sent to the Marketplace must have a cover sheet that is clearly labeled with the consumer’s name and account number (ACXXXXXXXXXXX).

• Each fax must contain documents for one (1) account holder only.

• For example: If an Assistor has two separate clients and needs to fax a one-page document to the Marketplace for each client, the Assistor must prepare two (2) separate faxes with separate cover sheets.

• If Identity Proofing remains pending after faxing in the consumer documents and the Assistor has not received a call from NY State of Health within 48 business hours, they should follow up with the dedicated identity proofing phone number at 1-855-357-8450.
Faxing Documents to the Marketplace

• The fax coversheet for Identity Proofing documents can be downloaded from the Assistor Toolkit website. Go to Assistor Resources. 
  https://info.nystateofhealth.ny.gov/assistortoolkit

• Assistors can type into the Fax Coversheet so that the information is easy to read and will be correctly linked to the client’s account.

• All of the instructions for faxing the marketplace are included on the fax coversheet.
UPLOADING DOCUMENTS TO THE MARKETPLACE

Consumer documents that contain PII (i.e., paystubs or immigration documents) must be uploaded separately by document type and consumer.

- For example: If one consumer has provided four paystubs related to her application, the Assistor should upload them together as one (1) upload. If this consumer is also providing their Permanent Resident Card to verify immigration status, the front and back of the card should be uploaded separately as one (1) upload.

Before uploading each document, an Assistor should check at least three (3) different elements of PII in the document (if available) against the account, to verify that the document matches the account.

- For example: Before uploading paystub copies, the Assistor should verify that the name, address and last four digits of the SSN on each paystub match the name, address and last four digits of the SSN on the account.

- **NOTE:** The type of PII in individual documents will vary. The important thing is to check at least three (3) different types of PII (if available) on each document to validate that the document matches the account.
Type of document being uploaded.

Name of the Account Holder
- Account Holder’s name will appear even if uploading documents for a household member, such as a child or spouse.

Best Practice:
Scroll down to view the entire page of the document.

Best Practice:
Check to make sure all pages were uploaded.

Type in the consumer’s Account Number to validate.
NYSOH Mobile Upload App

The NYSOH Upload App allows consumers to use a mobile device to submit their own documents to NY State of Health.

To find the NYSOH Upload App in the App Store® or in Google Play™:
1. Search for ‘NYSOH Upload’ App and look for our icon.
2. Download for free.

NYSOH Mobile Upload is quick and easy to use: the consumer needs to log in on a phone or tablet, choose the document from a list, snap a photo, and hit send.
NYSOH MOBILE UPLOAD APP, CONTINUED

• Once the consumer uploads their document using the app, they get a confirmation email. If they choose, they can also receive a text message once the document has been processed.

If the consumer wants to receive a text message, select “Yes” here.

• Assistors are permitted to help consumers download and use the NYSOH Upload App.
AUTHORIZED REPRESENTATIVES

• Assistors must explain to consumers that the Marketplace takes every precaution to maintain the privacy and security of their information.

• Assistors and the Call Center cannot give information out to individuals who have not been designated as an Authorized Representative (AR) by the account holder and that person has been identity proofed.

• Identity verification protects the account holder, and everyone else who is listed on the account, from unauthorized access.
AUTHORIZED REPRESENTATIVES, CONTINUED

- Assistors may explain the process to designate an AR and inform the consumer that this includes a family member, friend, lawyer or other trusted person.
- Consumers may also add an AR to their account as part of their online application. This functionality can be accessed by having the consumer log into their account independently (not from the Assistor dashboard), or by calling the Call Center.
- There are two types of ARs that the consumer can add to their account:
  - **24 Hour ARs** - Will not be required to be identity proofed.
    - Have access to a consumer’s account for 24 hours (from when access is granted) or until consumer chooses to end access (before 24 hours expires).
  - **Permanent ARs** - Will be required to be identity proofed.
    - Have indefinite access to a consumer’s account (until the consumer chooses to end the access).
**Authorized Representatives, Continued**

- Assistors can present the “Combined Authorized Representative Designation and Authorized Representative Identity Verification Form”.

- The Assistor may help the consumer complete the forms:
  - Schedule another appointment (if needed) to gather identity proofing documents for the AR and fax the forms to the Marketplace.
  - OR
  - Advise the consumer on how to fax or mail the documents to the Marketplace themselves (if they don’t have the appropriate documents available during their appointment).

  - In this scenario, the Assistor should take the time to review the forms and all the instructions on the forms with the consumer, to ensure that they understand the entire process and what documents will be acceptable.
AUTHORIZED REPRESENTATIVES, CONTINUED

- Authorized representative forms and accompanying documentation can be sent to:
  - Fax: 1-855-900-5557.
  - These forms cannot be uploaded at this time.

- Assistors should contact the Call Center to find out if the forms have been successfully processed and gain permission to work directly with the AR.
  - **NOTE**: It could take 7 to 10 business days for the form and documents to be processed by the Call Center.
  - If an AR is permanently assigned to an account, they will remain authorized on that account, even if the Assistor changes, until/unless the consumer un-authorizes them.
Emily and Xiao have been divorced for 5 years and share custody of their only child, Sam. Emily is the account holder and wants to change Sam’s health insurance to another plan but is unable to call or email due to her busy work schedule. Xiao has emailed you for assistance and information on plan options for Sam. How do you proceed with helping Xiao?
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

- HIPAA is a federal law passed in 1996 and amended by another federal law, passed in 2013, called HITECH.

- The actual rules are contained in federal regulations that have been in effect since 2003 (45 CFR Parts 160 and 164).

- Significant amendments to HIPAA went into effect in 2013, strengthening privacy and security provisions.
HIPAA: Covered Entities

HIPAA applies to certain types of organizations, called “Covered Entities.”

Covered Entities include:

- Health Care Providers, such as physicians and hospitals.
- Health Insurance Plans, such as Medicaid and Insurance Companies.
- Health Care Clearinghouses, which refers to companies that assist with claims processing or billing.

The Marketplace is a Covered Entity (specifically, a “Covered Program”) of the New York State Department of Health.
PROTECTED HEALTH INFORMATION

Under HIPAA, PII combined with “Health Information” (information about a person’s health care, including payment for health care) is “Protected Health Information” or “PHI.”

An individual consumer’s enrollment in a health plan is PHI.
INFO CHECK

• Account Numbers (AC0000000000)
• HX IDs (HX0000000000)
• Confirmation Numbers
• Other Stand-Alone Information

When they stand alone, they are not traceable, but as soon as they are combined with any other PII, they should be treated as protected information.
Business Associates

Many Assistors are “Business Associates” of the Marketplace under HIPAA, which means that they receive or transmit PHI on behalf of a Covered Entity (the Marketplace).

Business Associates have a Business Associate Agreement (BAA) with the Marketplace.

The HIPAA amendments that went into effect in 2013 included important changes for Business Associates. The federal Office of Civil Rights in the Department of Health and Human Services can take enforcement action directly against Business Associates for breaches of security or privacy.
HIPAA includes a Privacy Rule and a Security Rule that requires Covered Entities and Business Associates to use operational, administrative, technical and physical safeguards to prevent unauthorized access, use or disclosure of PHI.

Whether a consumer participates in the Medicaid program or any other health insurance program, that information is PHI that may only be used for Marketplace program purposes.

Assistors may only use PHI for Marketplace program purposes. It may not be disclosed or shared.
MEDICAID CONFIDENTIAL DATA AND UNEMPLOYMENT INFORMATION

• In addition to HIPAA, individually identifiable Medicaid Confidential Data is also protected by Federal and State Laws.

• An individual’s application for or receipt of Unemployment Insurance (UI) benefits is confidential information protected under Federal and State Laws.

• HIPAA adds to these protections, it does not replace them.
LIMITATION OF ACCESS

• Only Assistor staff who need access to PII / PHI to perform their assigned job responsibilities may have access (also known as “need to know”).

• Access to PII / PHI must be limited to what is minimally necessary for staff to do their jobs (also known as “minimum necessary”).

Unless a staff person has an assigned job responsibility, he or she should not have access to PII or PHI.
Poll Question #1

You just finished with a client appointment and notice that he left a handwritten piece of paper on your desk. The paper contains a passport number and email address. Is this considered PII?

A. Yes

B. No
If an Assistor suspects there has been a loss or potential loss of PII or PHI, including an unauthorized use or disclosure, he/she must *immediately* report it to a supervisor.

Assistor organizations must promptly report to the Marketplace any loss or potential loss of PII or PHI.

Assistor organizations must report any unauthorized access to or loss or suspected loss of any PII or PHI within 24 hours to:

- NYSOHSecurity@health.ny.gov
- (518) 457-3849
**HIPAA: Security Rule**

- Assistors must take steps to prevent unauthorized access to PHI.
  - Be aware of your surroundings while handling or discussing PII or PHI.
  - Use screen protectors if needed.

- Laptops used by Assistors to collect and transmit PII and PHI must be encrypted.
What is Disk Encryption?

- Encryption converts data into an unreadable format. In order to convert it back to an intelligible format, it needs to be unlocked with the secret key.
- Encryption refers to whole-disk encryption, which requires an Assistor organization to use software, such as Bitlocker, to encrypt the hard drive of the laptops that it provides to individual Assistors.
- If an *encrypted* laptop is lost or stolen, the data on the hard drive is unreadable.
- It is important to check with your supervisor to be sure that any laptop that has been given to you to provide Marketplace enrollment assistance is encrypted.
SECURITY BASICS

Protect your laptop and/or workstation.

1. Protect your User IDs and your passwords.
   • Change them frequently.
   • Do not post where they are visible to others.

2. Never let anyone else use your User ID and Password.

3. Use up-to-date anti-virus software and keep operating systems updated and patched with the latest security updates.

4. Always lock your computer when you leave your desk so that PII/PHI are not visible on the screen or accessible.

5. Secure any paper PII/PHI. Never place PII/PHI in a standard recycling bin or trash can.

6. Shred PII/PHI when finished with it, or store securely.
WHAT NOT TO DO

Assistors should NEVER:

• Discuss PII/PHI with co-workers who do not have a “need to know.”

• Discuss PII/PHI via telephone or provide enrollment assistance via telephone unless authorized by the Department of Health.
  o Unless speaking to a representative of NY State of Health or its Customer Service Center.

• Transmit PII/PHI via email.
  o Except in limited circumstances when Assistors need to send PII/PHI to a DOH staff member and only in an encrypted format.

• Discuss PII/PHI with a non-authorized person.
## SECURITY BASICS: PUBLIC LOCATION

<table>
<thead>
<tr>
<th>Problem</th>
<th>Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shoulder Surfers</td>
<td>Choose a space within your public location that is least subject to your computer screen being viewed by others.</td>
</tr>
<tr>
<td>Eavesdroppers</td>
<td>Encourage consumers to be aware and speak quietly when providing information.</td>
</tr>
<tr>
<td>Non-reading Consumers or Interpreters</td>
<td>Set the tone; let them know that it may be beneficial to move to a secure location or explain that you will be speaking quietly when reviewing PHI/PII.</td>
</tr>
<tr>
<td>PHI/PII Disposal</td>
<td>Encourage consumers to take responsibility for their own documents and dispose of them in a non-public location.</td>
</tr>
</tbody>
</table>
**Poll Question #2**

An investigator with a local law enforcement agency contacts your organization. She is demanding the current address and other PII for a specific consumer be faxed to her immediately for a high-profile case. Are you required to give her this consumer’s PII?

A. Yes

B. No

Contact your organization’s legal department or senior manager.

The Assistor Agency must report the inquiry to us at the Department of Health: NYSOHSecurity@health.ny.gov
What is Ransomware?

- Type of Malware.
- Typically Spread Through Phishing Emails.
- Encrypts and Locks Files.
- Holds Files for Ransom.

How do I get Ransomware?

- Spam and Phishing Emails.
- Malicious Web Advertisements.
- Unpatched Vulnerabilities.
**RANSOMWARE**

Your personal files are encrypted

**Info**

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by clicking on *see files* and try to open them.

Encryption was produced using **unique public key RSA-4096** generated for this computer. To decrypt files, you need to obtain **private key**.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.

**To retrieve** the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

**Any attempt to remove or damage this software will lead to immediate private key destruction by server.**
MARKETPLACE INFORMATION
SECURITY

• Never save or copy PII and PHI to mobile devices, such as flash drives or portable disk drives.

• Never photograph consumer documents for the purpose of uploading to an account.

• PII and PHI must not be stored on a laptop or PC.
  o You may retain a list of client names and phone numbers for the purpose of calling to make appointments, but no further client information should be saved on an Assistor’s work or personal computer, phone, or other devices.

The next three slides provide instructions on how to securely open a consumer’s notice and how to delete it from your computer if needed.
VIEWING NOTICES IN DIFFERENT BROWSERS

When you open and view a consumer notice, there are different steps you need to take to view the notice securely and delete it, if needed

• If possible, click on “Open” and not save.

• You may also check the box for “Do this automatically from now on”, click “OK”.

• Sometimes a notice automatically downloads a PDF to your computer. When you click the options arrow, you can either open the PDF or ‘Show in folder’ to see where the document has been saved on your computer. Follow this file path (usually a Temporary or Download file) to delete the notice from your computer.
MARKETPLACE E-MAIL RESTRICTIONS

• Assistors must NOT send PII and/or PHI via e-mail.
• Assistors must instruct consumers not to send PII or PHI to the Assistor organization via e-mail or text.
• Consumers should never text photos of documents.
• If an Assistor receives unsolicited PII from a consumer, they should send the consumer a reply letting them know that in the future, the consumer must:
  o Mail their document to the Assistor; or
  o Deliver their document to the Assistor agency in-person in a sealed envelope; or
  o Fax their document to the Assistor.
• Unsolicited e-mail/PII received from a consumer should be deleted from the e-mail account and then deleted from “trash.”
ENCRYPTED E-MAIL

In limited, time-sensitive circumstances, an Assistor may use encrypted e-mail to send PII or PHI as an encrypted attachment to specific DOH staff members with a need to know.

• PII and PHI must NEVER be sent in the body of an email.
• Assistors may send encrypted attachments in an e-mail, encrypting Microsoft Office (e.g., Word) attachments by password protecting, or using “WinZip” or “7Zip.”
• Passwords or “keys” to the encrypted file must be sent in a separate e-mail.
• To encrypt using Word, Excel or PowerPoint file click File > Info > Protect Document > Encrypt with Password.
Poll Question #3

What measures can you take to help prevent becoming a casualty of ransomware?

A. Backup your data.
B. Update and patch your systems.
C. Ensure your security solutions are up to date.
D. All the above.
SCENARIO #2

You have been Mrs. Smith's Assistor for the past 11 months. You have an appointment with her, and she is asking questions about her renewal notice. In the process of getting Mrs. Smith's renewal notice from the dashboard, you save the document to your computer.

How do you proceed?
SANCTIONS

Individuals who do not comply with Privacy & Security requirements may be subject to fines and other penalties.

- Any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the Affordable Care Act will be subject to a civil penalty of not more than $25,000 per person or entity, per use or disclosure, in addition to other penalties that may be prescribed by law.
HIPAA and HITECH Penalties

HITECH stands for Health Information Technology for Economic and Clinical Health

- The Health and Human Services (HHS) Office for Civil Rights may assess penalties against Covered Entities and Business Associates for failing to appropriately safeguard PHI. Penalties may be assessed per violation.

- Covered entities and individuals who knowingly obtain or disclose PHI may be subject to a fine of up to $50,000 and up to one (1) year in jail.
The Marketplace and its Assistors are subject to privacy and security rules protecting **PII**, in addition to the requirements of HIPAA governing PHI.

PII and PHI must be always safeguarded, including:

- Keeping PII and PHI confidential and disclosing it only as necessary to perform Assistor services.
- Using physical, operational, technical and administrative safeguards to protect the security of PII and PHI, including the encryption and secure storage of laptops.
- Never sending PII or PHI by standard e-mail.
- Checking at least three (3) elements of PII in each document (if available) against the account before uploading.
- Reporting any potential privacy or security concern promptly.
- Reviewing the security controls that are in place regularly and updating as needed.
Poll Question #4

It has been decided that a newly hired Assistor will cover your workload for five (5) days while you are on vacation. Are there any concerns that you should have about this?

A. No. She can access your Assistor Dashboard using your account, in order to work with your clients while you are away.

B. No. She has her own dashboard and can work with the consumer and the call center to transfer authorization on the consumer accounts as needed, while you are away.

C. Yes. She will not be able to assist your consumers.
CONTACT INFORMATION

Report any unauthorized access, loss or suspected loss of any PII or PHI to NYSOH Security within 24 hours.

NY State of Health Information Security Office

• Email: NYSOHSecurity@health.ny.gov

• Telephone: (518) 457-3849
QUESTIONS?
EMAIL CONTACTS

All Assistors

• If you have general Assistor training questions, or questions about this specific training, please send them to: Eligibility.Training.Support@health.ny.gov.

• If you have a case specific question that you have already discussed with your supervisor or program manager, the issue should be submitted on an encrypted Account Review Spreadsheet to: Assistor.Cases@health.ny.gov.

• If you need help with your Assistor account or Oversight Manager account, or if your agency needs to report staff changes, please send an email to: Assistor.Admin@health.ny.gov.

Navigators Only

• When Navigator Agencies are submitting contract documents (vouchers, annual packet documents, progress reports, site schedules, etc.) and related questions to the New York State Department of Health, please send them to: Navigator.Admin@health.ny.gov.
  o CC your Navigator Contract Manager

• When Navigator Agencies are submitting media approval requests, educational and marketing material approval requests, and consumer story submissions to the New York State Department of Health, please send them to: Navigator.Media@health.ny.gov.
  o CC your Navigator Contract Manager
**Recertification Process**

- All Assistors and Assistor Oversight Managers who are registered or completed the online Assistor certification training by **10/31/2021** will be required to view the recertification webinars. The material included in each webinar is a supplement to what was provided during the in-person and online courses.
  - [https://info.nystateofhealth.ny.gov/SpringTraining](https://info.nystateofhealth.ny.gov/SpringTraining).

- Keep track of the date you watched the live webinar or the video for each of this year’s six (6) recertification webinars.

- Provide your dates to your supervisor so they can complete the Recertification Report.
THANK YOU FOR JOINING US!

• Please complete the survey:
  o Privacy and Security webinar evaluation
• As always, watch for the video and materials to be posted to: http://info.nystateofhealth.ny.gov/SpringTraining.

Next Recertification Training:
Cultural Humility and Race and Ethnicity Application Changes

• Guest Speaker: Tekisha Dwan Everette, Ph.D
• Date: August 25, 2021
• Time: 2:00PM – 3:30PM