NEW YORK
STATE OF
OPPORTUNITY.

Office for
the Aging

# New York State Office For the Aging Health Insurance Information Counseling Assistance Program (HIICAP)

# Protecting Client Privacy and Confidentiality

July 14, 2023

# Training Objectives

- Define confidentiality and its implications for SHIP & SMP counseling work.
- Examine relevant confidentiality laws, policies, and implementation for SHIP & SMP operations.
- Identify best practices.
- Set expectations.
- Meet CMS Unique ID training requirements.

# What is “confidentiality?”

- To “confide” means to trust in someone.
- Especially when sharing secrets or private matters.
- “Confidence” means firm belief, trust, reliance.
- Belief that another person will keep a secret, or “maintain strict confidence.”
- “Confidential” means entrusted with private or secret matters.
- It’s about building and maintaining trust!

# Why is Confidentiality Important in HIICAP Work?

- It frees clients to share personal information that counselors need to do their work.
- It shows respect for and helps protect clients.
- It builds the program’s reputation as a trusted, reliable resource.
- It helps prevent costly privacy and security breaches (e.g., legal fees and fines).

# What Rules Affect Confidentiality in HIICAP Work?

- Federal law
- HIPAA (Health Insurance Portability and Accountability Act of 1996)
- Privacy Rule: privacy rights and access to records
- Security Rule: data protection duties and penalties
- State law
- Constitutional privacy rights in some states
- Privacy (data breach) acts
- Agency policies
- Volunteer Risk & Program Management (VRPM) Policies
- CMS Unique ID for SHIPs and SMPs

# HIPAA’s Two Parts

**The HIPAA Privacy Rule**

- Defines “protected health information,” or P.H.I.
- Establishes permitted uses & disclosures of P.H.I.
- Regulates authorized uses of P.H.I
- Limits uses and disclosures to minimum necessary.

**The HIPAA Security Rule**

- Addresses safeguards for “electronic protected health information,” or e-P.H.I.
- Requires covered entities to ensure confidentiality and integrity of all e-P.H.I.
- Identifies and protects against anticipated security threats.
- Protects against anticipated impermissible uses or disclosures.
- Ensures compliance by their workforce through training and oversight.

# Who does HIPAA Apply To?

- “Covered Entities” and their business associates must comply with HIPAA’s Privacy and Security Rules
- Health plans
- Includes Medicare, Medicare health plans, Medicaid, Medicare supplement insurers (Medigap), group health plans
- Health care providers
- Hospitals, nursing facilities, physicians, etc.
- Health care clearinghouses
- Billing services, health management information systems
- Business associates
- A person or organization that contracts with a covered entity to perform some of its functions

# Does HIPAA Apply to HIICAP?

The programs are not “covered entities” but…

- Local cosponsors may be covered entities if they provide health care services or contract with those who do.
- The U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) oversees and enforces HIPAA compliance. HIICAPs can help clients submit complaints about suspected violations to OCR: www.hhs.gov/ocr .
- Most third parties with whom HIICAPs interact are covered entities (i.e., Medicare, Medicare Advantage plans, hospitals, doctor offices, 1-800-MEDICARE, etc.)

# What is the HIPAA Privacy Rule?

- It’s a federal law that protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

- This information is called "protected health information,” or P.H.I.

# Individually Identifiable Health Information

“Individually identifiable health information” is information, including demographic data, that relates to:

- An individual’s past, present or future physical or mental health or condition,
- Providing health care to the individual, or the past, present, or future payment for Providing health care to an individual, and,
- Identifies the individual or gives a reasonable basis to use in identifying an individual.
- Individually identifiable health information includes common identifiers like name, address, birth date, Social Security Number.

# HIPAA Privacy Rule Protections

**Purpose:**

- The Privacy Rule defines and limits the circumstances when covered entities may use or disclose an individual's P.H.I.

**Basic Principle:**

- Covered entities may not use or disclose P.H.I. except as:
- The Privacy Rule requires or permits, or
- The individual/patient (or personal representative) authorizes in writing.

# Required Disclosures

The Privacy Rule requires covered entities to disclose P.H.I. in only two situations:

- To individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and
- to the Department of Health & Human Services (HHS) when it undertakes a compliance investigation or review, or an enforcement action

# Permitted Disclosures

- The Privacy Rule permits covered entities to use and disclose *P.H.I.*, without an individual’s authorization, in the following situations:
- To the individual (unless required for access or accounting of disclosures),
- For treatment, payment, and health care operations,
- Basis for the CMS Unique ID system,
- When the individual would have an opportunity to agree or object if not incapacitated,
- Incident to an otherwise permitted use and disclosure,
- For public interest and benefit activities, and
- For research, public health or health care operations in a limited data set.

# Privacy Rule Protections

An individual has rights under the Privacy Rule to:

- Receive notice about a provider’s privacy practices
- Review and obtain a copy of their P.H.I. in a covered entity’s designated record set
- Have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete
- An accounting of P.H.I. disclosed by a covered entity
- Request a covered entity to restrict P.H.I. disclosure
- Request alternate means or location for receiving communications of P.H.I., other than those typically used

# What is the HIPAA Security Rule?

It covers P.H.I. that is created, received, maintained or transmitted in an electronic form. This includes P.H.I.:

- Transmitted over the Internet (e.g., email)
- Stored on a computer, a CD, a disk, magnetic tape, or other related means.
- Stored on personal devices (e.g., cell phones and tablets)
- The Security Rule does not cover P.H.I. that is transmitted or stored on paper or provided orally.

# Security Rule Safeguards

Covered entities must protect against reasonably anticipated threats to, and impermissible uses and disclosures of P.H.I. by:

- Conducting risk analyses
- Implementing administrative safeguards
- Building physical safeguards
- Installing technical safeguards
- Documenting Policies & Procedures

# HIPAA: HIICAP Operations

Covered entities, including health care providers, can’t disclose an individual’s P.H.I. without written consent or the individual’s presence and oral consent.

- Use consent forms to document authorization
- Make 3-way calls with provider and client on the line

Customer service representatives at 1-800-MEDICARE can’t discuss a client’s P.H.I. with third parties

- Must use CMS Unique ID to conduct SMP and SHIP work
- Privacy training required

Electronic transmissions containing P.H.I. must be secure

- Use email encryption

HIPAA Security Rule is model for Volunteer Risk & Program Management  Information Technology (IT) policies

# State Law

- State Privacy Protection Laws
- Apply to individuals and organizations, including non-profit agencies
- Define “personal protected information,” or P.P.I.
- Prescribe process for notifying people affected by a security or data breach
- Some establish a statutory duty to protect personal information
- Some set fines for breaches

# What is Personal Protected Information (P.P.I.)?

- A beneficiary’s first name and last name or first initial and last name in combination with at least one of the following:
- Social Security number
- Driver’s license number or state-issued identification card number
- Financial account number or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account
- Protected personal information does not, however, include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public

# P.P.I. = P.I.I. and P.H.I.

**Personally Identifiable Information (P.I.I.)**

- Information which can be used to 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 which is linked or linkable to a specific individual, such as a data and place of birth, mother’s maiden name, etc.”1

**Protected Health Information (P.H.I.)**

- Individually identifiable health information that is explicitly linked to a particular individual, and health information which can allow individual identification.2

- P.H.I. includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

1.See www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf Safeguarding Against and Responding to the Breach of Personally Identifiable Information to more details.

2.Health Insurance Portability and Accountability Act of 1996. See website for more details at: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected

# What is a security breach?

Security breaches occur when unauthorized persons gain access to P.P.I./P.H.I. by:

- Stealing computers and/or computing files
- Overhearing conversations about clients
- Dumpster diving for medical and payment records
- Reading documents left on unattended desks or copy machines
- Extracting data from the hard drives of discarded copy machines
- Any other means

# VRPM Confidentiality Policy

What is the policy for protecting client confidentiality?

- Policy 3.94: SHIP & SMP volunteers are responsible for maintaining the confidentiality of all proprietary or privileged information to which they are exposed while serving as a volunteer, whether this information involves a member of staff, a volunteer, a beneficiary or other person, or involves the overall business of the SHIP.

# VRPM Confidentiality Policy, cont.

How does Policy 3.94 affect SHIP & SMP operations?

- Volunteers are to be trained on confidentiality before they get a CMS Unique ID
- Volunteers are to sign a written confidentiality agreement
- The agreement informs volunteers that a confidentiality breach is grounds for immediate dismissal
- Participation in SHIP & SMP is conditioned on full compliance with the agreement.

# Confidentiality Best Practices

- Volunteers take steps needed to safeguard beneficiary related information and prevent unauthorized persons from accessing P.P.I./P.H.I.
- Use private spaces in meetings with clients to ensure confidentiality
- Store documents containing P.H.I. in locked offices or filing cabinets
- Use computer screen covers to block PPI/P.H.I. from unauthorized viewers
- Shred written notes when no longer needed

# Confidentiality Best Practices, cont.

- Volunteers use information obtained in the course of their work only to assist the client or otherwise meet their responsibilities. They do not disclose confidential information to others unless authorized.

- Discuss cases with other SHIP & SMP staff in private

- Limit information sharing to minimum needed to assist, train, or report

- Return original documents containing P.P.I./P.H.I. to clients and make copies only when necessary

- Follow protocols to destroy documents containing P.P.I./P.H.I.

# VRPM IT Policies

- Volunteers are to comply with Information Technology (IT) procedures or protocols for:
- Controlling access to and use of beneficiary information
- Safe operation of computers used to collect and store program and beneficiary information
- Using the Internet, including e-mail use and appropriate access to web sites.
- Using wireless devices to connect to the Internet while performing SHIP or SMP work
- Using their personal computers while performing SHIP or SMP work.

# VRPM IT Policy Best Practices: Don’t

- **Don’t** send or forward e-mails with P.P.I. to personal e-mail accounts (e.g., Yahoo, Gmail).
- **Don’t** upload PPI to unauthorized websites (e.g., wikis).
- **Don’t** use unauthorized mobile devices to access P.P.I.

# VRPM IT Policy Best Practices: Do

- **Do** store PPI in a password protected file on a password-protected computer to which only authorized persons have access.

- **Do** report lost or stolen client information to your supervisor.

- **Do** lock your computer anytime you step away to avoid the chance that an unauthorized individual will access it.

- **Do** clear your web browser history to avoid other users accessing PPI.

- **Do** lock up portable devices (e.g., laptops, cell phones).

- **Do** use strong passwords, ideally “pass phrases,” for email accounts.

# Best Practice: Strong Passwords

- Strong passwords include a random combination of 8 or more numbers, symbols, capital and lower-case letters. Using different character types makes it harder for intruders  to crack the password.

- Pass phrase: Use an easily remembered phrase and substitute letters and numbers for words. Here’s an example of a pass phrase: “I Like To Sing and Take Long Walks” = 1L2$&Tlw.

# Password Do’s

- At least eight characters
- Special character (s): (%, ^, *, ?, <, >)
- Upper-case letter(s)
- Number(s)
- Lower-case letter(s)

# Password Don’ts

- Create easy-to-remember passwords.
- Use obvious passwords related to common information such as child’s or pet’s name, or your favorite sports team.
- Use passwords that someone can guess, using your social media information.
- Write down your password in a place that is accessible to others.
- Share your passwords.

# Best Practice: Wi-Fi Networks

Malicious actors could be lurking in the free Wi-Fi networks that you might use at your local coffee shop or while traveling.

Tips on the secure use of Wi-Fi

Use secured Wi-Fi networks such as your home Wi-Fi or Hotspot devices (mobile phone/tablet).

Do not access or transmit P.P.I. when using an unsecured Wi-Fi connection.

THANK
YOU!