HI PAA Compliance and Confidentiality Guidelines
Training Overview

- Knowledge refresher: terms and definitions
- Why do we take it seriously?
- The rules and standards to follow
- Contacts and Resources
Terms and Definitions

- HIPAA
- PHI
- “Use” vs “Disclosure”
What is HI PAA?

- HI PAA: Health Insurance Portability and Accountability Act of 1996
- It's a Federal Law
- Provisions of 1996 - 2013
- Protects privacy and security of patient/member information by addressing:
  - confidentiality
  - integrity
  - availability
What is PHI?

- PHI: Protected Health Information
- Any information related to an individual’s health status, treatment or payment for health services created or received by the organization that may identify the individual
- Includes: oral, written, and electronic records and communications
Question: Which of the following is PHI?

- A patient’s name.
- A patient’s email address.
- A patient’s health plan ID.
- A patient’s date of birth.
- A date of service.
- A medical record number, even if not linked to patient name.
- All of the above.
What is “Use”? 

USE means:
- Accessing
- Viewing
- Sharing
- Analysis of PHI within VNSNY
What is “Disclosure”?

DISCLOSURE means:

- Release
- Transfer
- Divulging

of PHI to an individual or entity outside of VNSNY
Confidentiality Practices
The Essence of The Privacy Rule

You **may not**

USE or DISCLOSE PHI

except as necessary to do your job.
Why to comply?

- It’s a Law, not an option
- Civil and Criminal Penalties may apply
- It is the right thing to do
Permitted Disclosures

- **Treatment**
  (providing healthcare to the participant)

- **Payment**
  (obtaining reimbursement for provided services)

- **Health Care Operations**
  (management functions required to run the plan efficiently)

- **All other uses:**
  participant must sign an authorization form
Other Permitted Disclosures* Without an Authorization

- To the U.S. Department of HHS
- For Legal, Regulatory and Law Enforcement Purposes
- Other (specifically addressed in HIPAA)

* When in doubt, contact the Privacy Officer, Privacy Liaisons or the Legal Department.
Participant Authorization

Must include:

- The PHI to be disclosed.
- People/entities who are permitted to disclose and receive PHI.
- The purpose of the disclosure.
- The termination date of the authorization.
- The patient’s or personal representative’s signature.
Minimum Necessary Rule

One must:

- Limit the participant information they use or disclose to the minimum necessary to accomplish their job responsibilities
- **Not** access, view, use, or disclose participant information unless they need it to do their job
Question: Is This a Violation?

A relative of a staff member is treated by your organization, and the relative asks the staff member to check on her lab work. It is easy for the staff member to look it up in the computer system. The staff member quickly checks on the lab work and tells her relative that everything looks good, but does not provide any details.

- No
- Yes
-Somewhat
Question: Is This a Violation?

A staff member emailed more PHI to other staff member than was necessary: the diagnosis information was not needed, but it was faster to “cut and paste” from a record.

- No
- Yes
- Somewhat
Participant Authorization and Minimum Necessary Rule

- Only release the information that is specifically authorized in the authorization (e.g., check that information to be sent complies with limitations on dates of service, as well as limitations on content).

- **It is a violation of the minimum necessary rule to send more information than is requested in response to a participant authorization.**
Prohibited Use and Disclosure

Staff may not:

- Discuss participants with fellow employees except as necessary for their jobs
- Carry participant information (written, electronic or oral) out of the office unless specifically authorized to do so
- Discuss participants information with family and friends
- Discuss PHI in elevators, lunchrooms or other common areas
Prohibited Use and Disclosure (cont.)

Staff may not:

- Talk or gossip about interesting participants, even if they see the participant’s story on the news
- Comment about participants on social media websites, even if a participant discloses health information on his/her own site
- Tell co-workers, friends or family about participants they may know
Work Station Protocol

A work station includes a desk or office of anywhere you set up your computer or do agency paperwork.

- Never leave PHI around in paper or electronic form - always keep it in a secure place
- If you leave your computer, lock it up or turn it off after securing all movable media
- In public areas, secure the monitor screen from prying eyes
- Don’t “post” PHI
- Don’t discard unneeded PHI in your own wastebasket - take it to shredder bin
Privacy Official

- Responsible for all matters related to our privacy practices
- Develops and implements required forms, policies and procedures
- Receives complaints about privacy violations
- Oversees compliance with HIPAA Privacy Rule
Policies & Procedures

- The Notice of Privacy Practices
- Participant Access to Medical Records
- Security Failure/ Breach
HI PAA, VNSNY Policies, and State Laws

- Follow VNSNY Confidentiality Policies
- If HI PAA and State Law address the same topic, HI PAA applies
- State Law applies if it offers participant greater rights
The Participant Notice of Privacy Practices
Notice of Privacy Practices

- How health information is used and disclosed
- Right to inspect and copy
- Right to request restrictions
- Right to request confidential communications
- Right to receive notification of breach
- Right to file a complaint
- Right to receive a copy of the Notice
Participant Access to Medical Records

Access to Individual Information Policy
Access to Individual Records

- **Participant is required to:**
  - Submit written and signed request

- **VNSNY CHOICE is required to:**
  - Append/upload written request
  - Respond within 30 days (10 days for providers)
  - Arrange convenient time
  - Charge copying fees (max. $0.75/page), postage fees
  - May provide a written summary in lieu of access per agreement with participant
Denial of Individual Access

- **Grounds for denial without review**
  - VNSNY is acting under direction of the correctional institution the participant is an inmate of
  - records are for use in legal or administrative proceedings
  - information obtained in ongoing research
  - information obtained from someone rather than a health care provider

- **Reviewable grounds**
  - PHI may endanger or make harm to the participant or other individuals as determined by a licensed health care professional
Disclosure to Personal Representative

- VNSNY may not treat a person as personal representative if participant is believed to be a subject of abuse.
- Any questions regarding access to health records by personal representatives, parents, guardians or other persons acting in loco parentis should be referred to VNSNY’s Privacy Officer or to VNSNY’s HI PAA attorney.
Security Failure/ Breach

- What is security breach?
- What are the consequences?
- What is the response?
Question: Is This a Security Breach?

A laptop with PHI is left in a car and stolen.

- No
- Yes
What are the consequences?

- Patient safety is compromised
- Negative publicity
- Costs
- Identity Theft
- VNSNY employee faces disciplinary action (policy)
- Legal liability
- Mandatory state and federal reporting of breaches
- Appointment of a government monitor to oversee compliance
How will VNSNY respond?

- Breach Determination
- Investigation
- Breach Notification
- Risk Assessment
- Mitigation
- Sanctions
For Reporting Suspected Violations

- 888-634-1558
- VNSNY CHOICE, 1250 Broadway NY, NY 10001
- CHOICECompliance@vnsny.org