Guidance from NYS to Health Homes on Protecting Personal Health Information (PHI)

All staff, volunteers, students, researchers, and consultants with access to Personal Health Information (PHI) must be trained on and comply with HIPAA privacy regulations.

Limit PHI shared with business associates by following a "minimally necessary" doctrine. Limiting PHI to the minimum necessary should still allow business associates to complete tasks and other work. *Use professional judgment and discretion.*

- Programs should protect the privacy of PHI by setting up administrative, technical and physical safeguards

- Program staff should safeguard—within reason—PHI from any intentional or unintentional use or disclosure

- Program staff should limit, whenever possible, the use/disclosure of PHI

- Protect your workstation
  - Lock your workstation when you leave your desk
  - Protect your user IDs
  - Ensure your passwords (work PC, laptops, palm devices, portable devices, flash drives, and home PC) are secure; change them frequently; do not save them; never tell anyone your passwords and never write them down
  - Use anti-virus software on PCs, laptops, etc.
  - Never let anyone else use your account
  - Minimize storage of PHI on your hard drive

- Verify identity of any person seeking PHI
  - Organizations should have verification policies and procedures
  - Ask for a combination of their address, SS#, birth date, maiden name, MA-ID#, etc.

- Know your organization's policies and procedures
  - Your organization should have a policy on laptop use as it relates to PHI
  - Use an encryption when sending data electronically or physically through the mail; never send PHI via e-mail unless it is encrypted in a password protected attachment
  - Make sure any PHI being faxed or e-mailed goes to the correct receiver, and that you include a confidentiality statement on the cover letter
  - Handheld devices and flash drives should have a policy that safeguards PHI

- Procedures for storage and use of individually identifiable information (18 NYCRR §357.5)
  - Mark documents as confidential
  - Keep confidential information in locked files/rooms
  - Access must be tied to specific job responsibilities

- Accessing PHI under federal regulations (45 CFR §§ 164.530, 164.502)
  - Staff can only access PHI when it is required for them to do their jobs
  - All staff volunteers, students, researchers, and consultants with access to PHI must be trained on and comply with HIPAA privacy regulations