Security and Privacy – Small Business Marketplace Policy and Procedures

Policy:

The NY State of Health works to ensure the protection of protected health information (PHI) and personally identifiable information (PII) in both internal and external communications by adhering to the following procedural guidelines. Business partners such as contracted vendors, participating insurance carriers, and assistors such as brokers and navigators are required to follow the same guidelines when communicating with NYS Department of Health (DOH) staff.

Definitions:

Personally Identifiable Information (PII) is information that can be used to distinguish a person's identity, such as their name, social security number or date of birth, when standing alone or when combined with other personal information, such as mother's maiden name.

•Name
•Social Security Number
•Date of Birth
•Mother's Maiden Name
•E-mail address
•Driver's license number
•Passport number
•Employer (*As stated below, AC number with employer's business name is okay to send via unencrypted email.)

Protected Health Information (PHI): 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."

Procedures:

- Encrypting Emails –
    - PII and PHI must not be transmitted via standard e-mail, such as Outlook. If it is necessary to transmit PII or PHI electronically to other DOH staff or business associates, it must be compressed and sent as an encrypted file using WinZip or 7Zip and labeled: Confidential, As Requested. The password or "key" to the encrypted file should be sent via separate e-mail marked: Regarding File.
        - Information including AC number only does not have to be encrypted

  - Sending information via email that includes an AC number along with an employer's business name is permitted, but any information including an employee's name or any other PHI or PII must be encrypted.
  - Password protecting a word document is not permitted in place of encryption.

- Do not copy PII or PHI on mobile devices such as flash drives or discs.

- Do not leave PII or PHI unattended in a printer or copier.

- Store documents containing PII or PHI securely when you are not using them.

- Promptly shred paper documents containing PII or PHI. Do not deposit in standard recycling bins.

- After the determination is made that data needs to be de-identified, determine which method of de-identifying the data will appropriately ensure this data cannot be inappropriately acquired.

- The following are acceptable methods to secure (de-identify) PHI in training manuals, Power Point Presentations, screen shots, etc.
  - Use a training environment
  - Create and use dummy data

- The following methods **are not** acceptable:
  - Printing screen shots and then using a marker to black out the data.
  - Placing a black text box over the PHI stored images within a word or excel document
  - Changing the font type to wing dings (Smith, Joe) or similar font type

- Reporting Procedures –

  - If a DOH staff person observes potential indications of a Security or Privacy concern, they should report it promptly as follows:

    - Do not investigate the incident on your own - immediately report suspected incidents that could compromise PII and PHI in any format (electronic, paper, or oral communications).

    - Inform supervisor and NY State of Health Security Team by completing the Security and Privacy Concern Form (see attached). Send the form promptly via encrypted e-mail to: NYSOH_securityandprivacy@csc.com, copying your supervisor.

- Do NOT include actual PII and PHI in the form.
- This form can be found in the Security and Compliance section of Sharepoint or request a form from the email above.
- For an immediate concern regarding the NYSOH System or Security, contact the CSC Command Center Incident Response number at 518-257-4215. This number is available 7-days a week.
- Staff can reference the NY State of Health Security & Privacy Quick Reference Guide for further guidance (see attached).
- There are several different circumstances or events that may be considered a potential issue or concern that should be reported, including:

  •A staff member receives an unencrypted email from a Qualified Health Plan with an enrollee's PII in the email (subject, body, or attachment).

  •An invoice from the Small Business Marketplace is mailed to the wrong address, and the mail is opened by the unintended recipient.

  •After working hours, PII is left unattended on a workforce member's desk, printer, or fax machine.

  •An email is sent into or out of the DOH system with PII that is not encrypted.

  •PII is accessed by a staff member without a Need to Know to complete assigned job responsibilities (i.e. access to a neighbor's PII).

  •Irregular activity involving the system (i.e. error or other odd message, email or document)

- It is important to remember that PII and PHI should be used only to complete assigned job responsibilities. If you have questions about privacy or security in your particular work area, be sure to speak to a supervisor.