SCHOHARIE ARC POLICY AND PROCEDURES

BOARD APPROVAL DATE:1/24/2020 EFFECTIVE DATE:1/24/2020

TITLE: HIPAA Hitech POLICY# 10-11

I. Policy

It is the policy of Schoharie Arc to protect the privacy and security of health information as required by federal HIPAA regulations and any other applicable laws or regulations. If a breach of protected health information (PHI) occurs, Schoharie Arc is required to provide notification to certain individuals and entities pursuant to Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH) and any regulations promulgated under the Act. This policy sets forth the procedures Schoharie Arc will follow to assess known and potential breaches of PHI and provide notification to affected individuals as necessary.

Definitions

Breach. For the purposes of this policy, the term "breach" means the acquisition, access, use or disclosure of unsecured PHI in a manner not otherwise permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

Protected Health Information (PHI). For the purposes of this policy, the term "PHI" means any program participant information, including very basic information such as their name or address, that (1) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (2) either identifies the individual or could reasonably be used to identify the individual.

II. Scope

This Policy applies to all employees, persons associated with the provider, executives and governing body members of Schoharie Arc.

III. Procedure

A. Reporting of Potential Breaches

Any employee, person associated with the provider, executive or governing body member who knows, believes or suspects that a breach of protected health information has occurred, must report the breach to the Privacy Officer or designee immediately. After a potential breach is reported, the Privacy Officer will work with other staff and departments including the HIPAA Security Officer, the information technology department, and in-house or outside legal counsel, if necessary, to determine if a breach requiring notification has occurred. As part of the investigation, the Privacy Officer will take all necessary steps to mitigate any known harm. The details of the investigation will be documented in an investigation report that is kept on file by the Privacy Officer. Information regarding breaches or potential breaches including internal/external reports of a breach, risk assessments as to possible harm, the investigation report, letters of notification to individuals, notice to media outlets, and the log of breaches to be reported to HHS, must be retained for a period of at least six (6) years.

B. Investigation of Potential Breaches

After a potential breach is reported, the Privacy Officer will conduct a thorough investigation to determine whether a breach of unsecured PHI requiring notification under HITECH has occurred. Schoharie Arc has 60 days from the date of discovery of the breach to make notifications, if required. If a breach under HITECH has occurred and notifications are required, the time period by which notifications must be sent to the affected individuals, HHS, and if necessary, the media, is measured from when the breach is first discovered, not when the Privacy Officer completes his/her investigation into whether a breach has occurred.

Not every report of a potential breach of PHI will result in the need to provide notification. The Privacy Officer will perform and document the following analysis:

- Determine whether there has been an impermissible acquisition, access, use, or disclosure of protected health information under the HIPAA Privacy Rule.
- Determine whether the PHI was "secure" or "unsecured".
- Determine whether an exception applies.
- Determine whether the impermissible acquisition, access, use or disclosure compromises the security or privacy of the protected health information.

1. <u>Was the acquisition, access, use, or disclosure impermissible?</u>

An impermissible acquisition, access, use or disclosure under the HIPAA Privacy Rule, is one in which one or more elements of the Privacy Rule have been violated. The Privacy Officer will investigate and determine if a provision of the Privacy Rule has been violated.

If the Privacy Officer determines that the acquisition, access, use, or disclosure was permissible under the Privacy Rule, no further investigation is required. If, however, the Privacy Officer determines that an impermissible acquisition, access, use, or disclosure has occurred, the investigation proceeds to step 2 below.

2. <u>Was the protected health information secured or unsecured?</u>

Breach notification will only be necessary under the HITECH rules where the breach involves "unsecured" PHI. PHI will only be considered secure, and thus exempt from the notification requirements, if it has been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS. HHS guidance on this issue states that PHI will not be considered secure unless it has either been (1) destroyed or (2) encrypted in accordance with specific standards approved by the National Institute of Standards and Technology (NIST).

While Schoharie Arc's use of firewalls, password protections/access controls and redacting meet the HIPAA Security Rule requirements, these methods do not adequately "secure" the PHI for HITECH purposes and they do not exempt Schoharie Arc from mandatory breach notification.

In most cases, Schoharie Arc's paper records containing PHI would be considered "unsecured PHI" and most of Schoharie Arc's electronic records would also be considered "unsecured PHI." Impermissible use or disclosure of these records would trigger the notification requirements under HITECH.

If the Privacy Officer determines that the PHI at issue is "unsecured", then the investigation proceeds to step 3 below.

3. <u>Does the breach fall under an exception to the notification rules?</u>

Schoharie Arc may not have to make notifications if the breach falls under one of the exceptions contained in the HITECH rules:

a) The acquisition, access, or use of PHI was by a workforce member, occurred in good faith and within the course and scope of employment or other professional relationship, and it does not result in further disclosure or use not permitted under HIPAA;

b) There was an inadvertent disclosure by an authorized workforce member to another authorized workforce member at the same covered entity or business associate, and there was no further disclosure or use not permitted under HIPAA; or

c) There is a good faith belief that the unauthorized person to whom disclosure of PHI was made would not reasonably have been able to retain the information.

If the Privacy Officer determines that none of the above exceptions apply to the impermissible acquisition, access, or use of PHI at issue, then the investigation must proceed to step 4 below.

4. <u>Is there a significant risk of financial, reputational, or other harm to the individual?</u>

If the Privacy Officer determines (1) that the acquisition, access, use or disclosure of PHI was impermissible; (2) that the PHI was unsecured; and (3) that no exception applies; then a risk assessment must be performed to determine if the breach will pose a significant risk of financial, reputational, or other harm to the individual(s) affected. The risk assessment must be documented in writing and the following factors must be considered:

- Who impermissibly used the information and to whom the information was impermissibly disclosed (there may be less risk if disclosed to another entity covered by HIPAA)
- Whether any immediate steps have been taken to mitigate an impermissible use or disclosure
- Whether the information is accessible and usable
- Whether the PHI disclosed was returned prior to being accessed
- The type and amount of PHI involved in the disclosure
- The risk of re-identification of PHI contained in a limited data set

If the Privacy Officer concludes that there is no significant risk of harm, then no breach notification is required, and the investigations stops. However, the Privacy Officer is responsible for determining if an "accounting" of the breach must be made in the records of the individuals affected and for determining if the breach notification provisions of any other state or federal law apply. If the Privacy Officer concludes that a reportable breach has occurred, notification to affected individuals, the Secretary of HHS and, if applicable, the media is required.

C. Breach Notifications

Notification must be provided to each individual whose unsecured PHI has been or is reasonable believed to have been acquired, accessed, used or disclosed as a result of the breach without unreasonable delay and no later than 60 calendar days after discovery of the breach. If the breach requires the involvement of law enforcement, the notification may be delayed for a period of time as determined by a law enforcement official.

1. <u>Notification Procedure</u>

Notification will be made as follows:

a. Schoharie Arc will notify the affected individual(s) via written first class mail. If necessary, Schoharie Arc will update the affected individual(s) through the mail as more information becomes known.

b. If Schoharie Arc does not have updated address information on an affected individual, a substitute method of notification is acceptable. In cases where there are 10 or more individuals for whom there is insufficient or out-of-date contact information, then Schoharie Arc will make a conspicuous posting on the homepage of its website.

c. In an urgent case where there is reason to believe an imminent misuse of the unsecured PHI, Schoharie Arc may make telephone and email notifications and follow up with mail notifications to the affected individual(s).

d. If the breach involves 500 or more individuals, Schoharie Arc will notify prominent media outlets serving the Schoharie Arc geographical service area.

e. In addition to the above, in the event of a breach affecting over 500 persons, Schoharie Arc will notify the Secretary of Health and Human Services no later than then when notice is provided to the affected individuals.

f. On an ongoing basis, Schoharie Arc will log all breaches affecting less than 500 individuals and submit the log annually to the Secretary of HHS.

2. <u>Content of the Notification</u>

To the extent possible, the notification must include the following elements:

a. A brief description of what happened, including the dates of the breach and of its discovery.

b. A description of the types of unsecured PHI that were involved in the breach (i.e., full name, Social Security Number, date of birth, home address, account number, procedure code, diagnosis, treatment, etc.)

c. What steps the individuals should take to protect themselves from potential harm.

d. What Schoharie Arc is doing to investigate the breach, mitigate losses, and protect against further breaches.

e. Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free number, an email address, web site or postal address.

3. <u>Annual Report to HHS</u>

Schoharie Arc will submit an annual breach notification report to the Secretary of HHS with information on any breaches of unsecured PHI involving less than 500 persons. All such reports must be submitted no later than 60 days after the end of the calendar year (by March 1st). Alternatively, Schoharie Arc may choose to file a report with the Secretary of HHS after the conclusion of each breach investigation rather than waiting until the end of the calendar year.

4. Notification by Business Associate

To the extent necessary, the agreements that Schoharie Arc has with it various business associates will be revised to require the business associate to notify Schoharie Arc of any breach of unsecured PHI. Schoharie Arc will require its business associates to notify Schoharie Arc of any known or suspected breaches within **[48 hours]** of discovery so that it may begin an investigation and meet its notification requirements within the 60 day period. The business associates notification must include the identity of each individual affected by the breach and any other information Schoharie Arc is required to include in it breach notification.

D. Training

1. All workforce members shall receive training on their responsibilities and obligations under HIPAA and HITECH during the orientation training process.
2. Refresher training shall be provided annually and whenever there are any changes to the regulatory requirements.
3. Training shall include information on how to prevent breaches of PHI as well as how to identify and report any breaches within the Agency.

E. Disciplinary Action

Schoharie Arc will apply appropriate disciplinary action against any employees, persons associated with the provider, executives and governing body members who fail to comply with this policy and procedure up to and including termination. Any employee, persons associated with the provider, executives or governing body members who knows or has reason to believe that another person has violated this policy is responsible for reporting the matter promptly to his/her supervisor and the corporate compliance officer.