The Guild for Exceptional Children
HIPAA Breach Notification Policy and Procedure

Purpose

To provide for notification in the case of breaches of "Unsecured Protected Health Information" ("Unsecured PHI") as defined under section 13402(h) of the HITECH Act ("Act"). The breach notification provisions of the Act apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose Unsecured PHI.

Policy

The Guild for Exceptional Children (GEC) will implement reasonable and appropriate technologies and methodologies designed to secure protected health information from unauthorized disclosure. "Unsecured PHI" means protected health information that is not secured through the use of approved technologies or methodologies. To be approved, technologies and methodologies must render protected health information ("PHI") unusable, unreadable, or indecipherable to unauthorized individuals, as described below.

If PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals, then the PHI is not "Unsecured PHI."

Procedures

1. <u>Methods of Protection</u> – Either of the following methods may be used to secure PHI and make it unusable, unreadable, or indecipherable to unauthorized individuals.

   (a) Encryption –GEC will implement and maintain reasonable and appropriate encryption technologies and methodologies to enhance the protection of PHI.[1]

   (b) Destruction –GEC will implement destruction techniques that render PHI unusable and/or unreadable in any format. [2]

---

[1] GEC currently uses Sonic Wall firewall protection and 64 bit encryption throughout the Agency's network, the separately maintained Agency server, and on all Agency computers.

[2] Data disposed, which includes discarded paper records or recycled electronic media: The media on which the PHI is stored or recorded is routinely destroyed in one of the following ways: Paper, film, or other hard copy media are shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed (See GEC Record Retention, Storage, & Destruction Policy). Redaction is specifically excluded as a means of data destruction. Electronic media are routinely cleared and purged using "CC Cleaner".

(c) If GEC fails to enforce security safeguards, the Agency may be subject to administrative penalties by the federal Department of Health and Human Services Office for Civil Rights.

PHI secured by one of the above methods of protection above is not unsecure and is therefore not subject to this policy.

For additional information on the guidelines and standards of encryption and destruction methods, contact the Security Officer.

2. <u>Breach Determination and Notification Process Steps</u>

(a) The Privacy Officer, with the assistance of the Security Officer and counsel, will determine whether a breach of Unsecured PHI has occurred and whether the event falls within the reporting requirements. In summary, the process steps to make this determination involve addressing these questions:

Step 1: Has Unsecured PHI been disclosed that violates the HIPAA Privacy or Security Rules?

Step 2: If yes, can the presumption that a breach has occurred be overcome because GEC can demonstrate that there is a low probability that the PHI has been compromised based on the risk assessment set forth below?

Step 3: If no, does the disclosure fall under an exception to the reporting requirements?

Step 4: If no, GEC will complete the notification and reporting requirements.

Step 1:

Upon receiving a report of a potential breach, the Privacy Officer, with the assistance of the Security Officer and counsel, will review the report to determine whether there has been an access, use or disclosure of Unsecured PHI by GEC personnel that violates the HIPAA Privacy or Security Rules.

Step 2:

If there has been a violation, a breach is presumed. The Privacy Officer, with the assistance of the Security Officer and counsel, will conduct a risk assessment to determine whether there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

Step 3:

If there is not a low probability that the PHI has been compromised, the Privacy Officer, with the assistance of the Security Officer and counsel, will consider whether there is an applicable exception to reporting, including:

- Any unintentional acquisition, access, or use of Unsecured PHI by GEC personnel, if done in good faith and within the scope of authority, and which does not result in further use or disclosure in a manner not permitted under the Privacy or Security Rule.
- Any inadvertent disclosure by a person from GEC authorized to access the Unsecured PHI to another person from GEC authorized to access the Unsecured PHI, and the Unsecured PHI is not further used or disclosed in a manner not permitted under the Privacy or Security Rule.
- Any disclosure where GEC has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Step 4:

If it is determined that: 1) a breach of Unsecured PHI has occurred, 2) there is not a low probability that the PHI has been compromised; and 3) no exception to the reporting requirement applies, GEC will notify each individual whose Unsecured PHI was breached. GEC will notify individuals as soon as reasonably possible after the Agency takes a reasonable time to investigate the circumstances surrounding the breach, but in no case later than 60 calendar days following discovery of the breach. The 60 days is an outer limit and therefore, in some cases, it may be an "unreasonable delay" to wait until the 60th day to provide notification. The notice of breach to individuals will include the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of Unsecured PHI involved in the breach (such as whether full name, social security number, date of birth,

home address, account number, diagnosis, disability code, or other types of information were involved);

- Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of the actions taken to investigate the breach, mitigate harm to individuals, and protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

GEC will provide the notice in written form by first-class mail to the last known address of each individual, or may provide written notice by electronic mail, if the individual agrees to receive electronic notice, and such agreement has not been withdrawn. If the affected individual is a minor or otherwise lacks legal capacity, the notification will be sent to the individual's Personal Representative. If the individual is deceased, the notice will be sent to the deceased individual's next of kin or Personal Representative if the address of the decedent's next of kin or Personal Representative is known.

If there is insufficient contact information for some or all affected individuals, individuals will be provided with a substitute notice. If sufficient contact information is unavailable for fewer than ten (10) affected individuals, substitute notice will be provided through an alternative form of written notice, such as electronic mail, telephone or other means. If no current contact information is available for the individuals, notice will be posted on GEC's home page in a manner that is reasonably calculated to reach the individuals.

If there is insufficient or out of date information for ten (10) or more individuals, substitute notice will be provided through a conspicuous posting on the home page of GEC's website or conspicuous notice in major print or broadcast media, for a period of 90 days. In addition, a phone number will be provided so that individuals can obtain more information about the breach.

If it has been determined that the breach of Unsecured PHI involved more than 500 residents of a particular state or jurisdiction smaller than a state, such as a county or city, GEC will notify a prominent media outlet of the breach. The Agency will determine whether media notification is required and if so, will cause such notification to be made. Notification to media may be made by issuing a press release.

If it has been determined that a breach gave rise to an urgent situation involving possible imminent misuse of the individual's information, GEC may provide notice by telephone or other means to individuals, in addition to direct written notice by first-class mail or email.

Relevant State laws will also be analyzed for additional requirements, including New York's Breach Notification Law, which applies to a breach of electronic information where "private" information is involved, including social security number, drivers license number, or account, credit or debit card number, in combination with any required security code or access code, or password that would permit access to an individual's financial account. This type of breach may require notice to the New York State Attorney General's Office and counsel should be consulted.

3. Tracking

(a) GECwill notify the Unites States Department of Health and Human Services ("DHHS") of all breaches of Unsecured PHI made by Agency personnel, either on an annual basis or immediately, depending upon how many individuals were affected by a breach. If a breach of Unsecured PHI involved more than 500 individuals, GEC will notify DHHS contemporaneously with the notification sent to an individual (within a reasonable time to investigate the circumstances surrounding the breach, but in no case later than 60 calendar days following discovery of the breach).

(b) Under the direction of the Privacy Officer, GEC will create and maintain a log of all breaches involving less than 500 individuals committed by Agency personnel. Within 60 days after the end of each calendar year in which the breaches were "discovered," GEC will submit the log to DHHS. The Agency will also maintain the log and all other documentation regarding breach of Unsecured PHI for six years. GEC is not required to submit information to DHHS for breaches that occurred before February 22, 2010.

4. GEC Personnel Reporting Requirements

(a) GEC personnel who discover, believe, or suspect that Unsecured PHI has been accessed, used or disclosed in a way that violates the HIPAA Privacy or Security Rules, must immediately report such information to the Privacy Officer.

(b) GEC personnel who are determined to have failed to adhere to the policies and procedures regarding reporting of the breach of Unsecured PHI will be subject to the disciplinary policies of the Agency.