Reportable Breach Notification Policy

I. Introduction

This Reportable Breach Notification Policy is adopted by the Plan as part of the Plan's Privacy Policy and is intended to comply with the final HITECH regulations at 45 CFR §164.400 et seq. for breaches occurring on or after September 23, 2013 ("Breach Regulations").

Under the Breach Regulations, if a Reportable Breach of unsecured protected health information has occurred, the Plan must comply with certain notice requirements with respect to the affected individuals, HHS, and, in certain instances, the media.

II. Identifying a Reportable Breach

The first step is to determine whether a Reportable Breach has occurred. If a Reportable Breach has not occurred, the notice requirements do not apply.

The Privacy Official is responsible for reviewing the circumstances of possible breaches brought to his or her attention and determining whether a Reportable Breach has occurred in accordance with this Reportable Breach Notification Policy and the Breach Regulations. All Business Associates, and all workforce members who have access to protected health information, are required to report to the Privacy Official any incidents involving possible breaches

Acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under the privacy rules is presumed to be a Reportable Breach, unless the Privacy Official determines that there is a low probability that the privacy or security of the protected health information has been or will be compromised.

The Privacy Official's determination of whether a Reportable Breach has occurred must include the following considerations:

- *Was there a violation of HIPAA Privacy Rules?* There must be an impermissible use or disclosure resulting from or in connection with a violation of the HIPAA Privacy Rules by the Plan or a Business Associate of the Plan. If not, then the notice requirements do not apply.
- *Was protected health information involved?* If not, then the notice requirements do not apply.
- *Was the protected health information secured?* For electronic protected health information to be "secured," it must have been encrypted to NIST standards or destroyed. For paper protected health information to be "secured," it must have been destroyed. If yes, then the notice requirements do not apply.
- *Was there unauthorized access, use, acquisition, or disclosure of protected health information?* The violation of HIPAA Privacy Rules must have involved one of these. If it did not, then the notice requirements do not apply.
- *Is there a low probability that privacy or security was compromised?* If the Privacy Official determines that there is only a low probability of compromise, then the notice requirements do not apply.

To determine whether there is only a low probability that the privacy or security of the protected health information was compromised, the Privacy Official must perform a risk assessment that considers 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.* For example, did the disclosure involve

financial information, such as credit card numbers, Social Security numbers, or other information that increases the risk of identity theft or financial fraud; did the disclosure involve clinical information such as a treatment plan, diagnosis, medication, medical history, or test results that could be used in a manner adverse to the individual or otherwise to further the unauthorized recipient's own interests.

- *The unauthorized person who used the protected health information or to whom the disclosure was made.* For example, does the unauthorized recipient of the protected health information have obligations to protect the privacy and security of the protected health information, such as another entity subject to the HIPAA privacy and security rules or an entity required to comply with the Privacy Act of 1974 or the Federal Information Security Management Act of 2002, and would those obligations lower the probability that the recipient would use or further disclose the protected health information inappropriately? Also, was the protected health information impermissibly used within a covered entity or business associate, or was it disclosed outside a covered entity or business associate?
- *Whether the protected health information was actually acquired or viewed.* If there was only an opportunity to actually view the information, but the Privacy Official determines that the information was not, in fact, viewed, there may be a lower (or no) probability of compromise. For example, if a laptop computer with was lost or stolen and subsequently recovered, and the Privacy Official is able to determine (based on a forensic examination of the computer) that none of the information was actually viewed, there may be no probability of compromise.
- *The extent to which the risk to the protected health information has been mitigated.* For example, if the Plan can obtain satisfactory assurances (in the form of a confidentiality agreement or similar documentation) from the unauthorized recipient of that the information will not be further used or disclosed or will be destroyed, the probability that the privacy or security of the information has been compromised may be lowered. The identity of the recipient (e.g., another covered entity) may be relevant in determining what assurances are satisfactory.

If the Privacy Official determines that there is only a low probability that the privacy or security of the information was compromised, then the Plan will document the determination in writing, keep the documentation on file, and not provide notifications. On the other hand, if the Privacy Official is not able to determine that there is only a low probability that the privacy or security of the information was compromised, the Plan will provide notifications.

If an exception applies, then a Reportable Breach has not occurred, and the notice requirements are not applicable.

- *Exception 1:* A Reportable Breach does not occur if the breach involved an unintentional access, use, or acquisition of protected health information by a workforce member or Business Associate, if the unauthorized access, use, acquisition, or disclosure-(a) was in good faith; (b) was within the scope of authority of the workforce member or Business Associate; and (c) does not involve further use or disclosure in violation of the HIPAA privacy rules. For example, the exception might apply if an employee providing administrative services to the Plan were to access the claim file of a participant whose name is similar to the name of the intended participant; but if the same employee intentionally looks up protected health information of his neighbor, the exception does not apply.
- *Exception 2:* A Reportable Breach has not occurred if the breach involved an inadvertent disclosure from one person authorized by the Plan to have access to protected health information to another person at the same covered entity or Business Associate also authorized to have access to the protected health information, provided that there is no further use or disclosure in violation of the HIPAA privacy rules. For example, the exception might apply if an employee providing administrative services to the Plan inadvertently emailed protected health information to the wrong co-worker; but if the same employee emailed the information to an unrelated third party, the exception likely does not apply.
- *Exception 3:* A Reportable Breach has not occurred if the breach involved a disclosure where there is a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the protected health information. For example,

the exception may apply to an EOB mailed to the wrong person and returned to the Plan unopened, or if a report containing protected health information is handed to the wrong person, but is immediately retrieved before the person can read it. However, the exception does not apply if an EOB was mailed to the wrong person and the unintended recipient opened the envelope before realizing the mistake.

III. If a Reportable Breach Has Occurred: Notice Timing and Responsibilities

If the Privacy Official determines that a Reportable Breach has occurred, the Privacy Official will determine (in accordance with the Breach Regulations) the date the breach was discovered in order to determine the time periods for giving notice of the Reportable Breach. The Plan has reasonable systems and procedures in place to discover the existence of possible breaches, and workforce members are trained to notify the Privacy Official or other responsible person immediately so the Plan can act within the applicable time periods.

The Privacy Official is responsible for the content of notices and for the timely delivery of notices in accordance with the Breach Regulations. However, the Privacy Official may, on behalf of the Plan, engage a third party (including a Business Associate) to assist with preparation and delivery of any required notices.

The Breach Regulations may require a breach to be treated as discovered on a date that is earlier than the date the Plan had actual knowledge of the breach. The Privacy Official will determine the date of discovery as the earlier of-(1) the date that a workforce member (other than a workforce member who committed the breach) knows of the events giving rise to the breach; and (2) the date that a workforce member or agent of the Plan, such as a Business Associate (other than the person who committed the breach) would have known of the events giving rise to the breach by exercising reasonable diligence.

Except as otherwise specified in the notice sections that follow, notices must be given "without unreasonable delay" and in no event later than 60 calendar days after the discovery date of the breach. Accordingly, the investigation of a possible breach, to determine whether it is a Reportable Breach and the individuals who are affected, must be undertaken in a timely manner that does not impede the notice deadline.

There is an exception to the timing requirements if a law-enforcement official asks the Plan to delay giving notices.

IV. Business Associates

If a Business Associate commits or identifies a possible Reportable Breach relating to Plan participants, the Business Associate must give notice to the Plan. The Plan is responsible for providing any required notices of a Reportable Breach to individuals, HHS, and (if necessary) the media.

Unless otherwise required under the Breach Regulations, the discovery date for purposes of the Plan's notice obligations is the date that the Plan receives notice from the Business Associate.

In its Business Associate contracts, the Plan will require Business Associates to-

- report incidents involving breaches or possible breaches to the Privacy Official in a timely manner;
- provide to the Plan any and all information requested by the Plan regarding the breach or possible breach, including, but not limited to, the information required to be included in notices (as described below); and
- establish and maintain procedures and policies to comply with the Breach Regulations, including workforce training.

V. Notice to Individuals

Notice to the affected individual(s) is always required in the event of a Reportable Breach. Notice will be given without unreasonable delay and in no event later than 60 calendar days after the date of discovery (as determined above).

A. Content of Notice to Individuals

Notices to individuals will be written in plain language and contain all of the following, in accordance with the Breach Regulations:

- A brief description of the incident.
- If known, the date of the Reportable Breach and the Discovery Date.
- A description of the types of unsecured protected health information involved in the Reportable Breach (for example, full name, Social Security numbers, address, diagnosis, date of birth, account number, disability code, or other).
- The steps individuals should take to protect themselves (such as contacting credit card companies and credit monitoring services).
- A description of what the Plan is doing to investigate the Reportable Breach, such as filing a police report or reviewing security logs or tapes.
- A description of what the Plan is doing to mitigate harm to individuals.
- A description of what measures the Plan is taking to protect against further breaches (such as sanctions imposed on workforce members involved in the Reportable Breach, encryption, installation of new firewalls).
- Contact information for individuals to learn more about the Reportable Breach or ask other questions, which must include at least one of the following: Toll-free phone number, email address, website, or postal address.

B. Types of Notice to Individuals

The Plan will deliver individual notices using the following methods, depending on the circumstances of the breach and the Plan's contact information for affected individuals.

Actual Notice will be given in all cases, unless the Plan has insufficient or out-of-date addresses for the affected individuals. Actual written notice-

- will be sent via first-class mail to last known address of the individual(s);
- may be sent via email instead, if the individual has agreed to receive electronic notices;
- will be sent to the parent on behalf of a minor child; and
- will be sent to the next-of-kin or personal representative of a deceased person, if the Plan knows the individual is deceased and has the address of the next-of-kin or personal representative.

Substitute Notice will be given if the Plan has insufficient or out-of-date addresses for the affected individuals.

- If addresses of fewer than ten living affected individuals are insufficient or out-of-date, substitute notice may be given by telephone, an alternate written notice, or other means.
- If addresses of ten or more living affected individuals are insufficient or out-of-date, substitute notice must be given via either website or media.- *Substitute notice via website.* Conspicuous posting on home page of the website of the Plan or Plan Sponsor for 90 days, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. Contents of the notice can be provided directly on the website or via hyperlink.
- *Substitute notice via media.* Conspicuous notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, including a toll-free number that remains active for at least 90 days where individuals can learn whether the individual's unsecured information may have been included in the breach. It may be necessary to give

the substitute notice in both local media outlet(s) and statewide media outlet(s) and in more than one state.
- Substitute Notice is not required if the individual is deceased and the Plan has insufficient or out-of-date information that precludes written notice to the next-of-kin or personal representative of the individual.

Urgent Notice will be given, in addition to other required notice, in circumstances where imminent misuse of unsecured protected health information may occur. Urgent notice must be given by telephone or other appropriate means.

- Example: Urgent notice is given to an individual by telephone. The Plan must also send an individual notice via first-class mail.

VI. Notice to HHS

Notice of all Reportable Breaches will be given to HHS. The time and manner of the notice depends on the number of individuals affected. The Privacy Official is responsible for both types of notice to HHS.

Immediate Notice to HHS. If the Reportable Breach involves 500 or more affected individuals, regardless of where the individuals reside, notice will be given to HHS without unreasonable delay, and in no event later than 60 calendar days after the date of discovery (as determined above). Notice will be given in the manner directed on the HHS website.

Annual Report to HHS. The Privacy Official will maintain a log of Reportable Breaches that involve fewer than 500 affected individuals, and will report to HHS the Reportable Breaches that were discovered in the preceding calendar year. The reports are due within 60 days after the end of the calendar year. The reports will be submitted as directed on the HHS website.

VII. Notice to Media (Press Release)

Notice to media (generally in the form of a press release) will be given if a Reportable Breach affects more than 500 residents of any one state or jurisdiction. For example:

- If a Reportable Breach affects 600 individuals who are residents of Oregon, notice to media is required.
- If a Reportable Breach affects 450 individuals who are residents of Oregon and 60 individuals who are residents of Idaho, notice to media is not required.

If notice to media is required, notice will be given to prominent media outlets serving the state or jurisdiction. For example:

- If a Reportable Breach involves residents of one city, the prominent media outlet would be the city's newspaper or TV station.
- If a Reportable Breach involves residents of various parts of the state, the prominent media outlet would be a statewide newspaper or TV station.
- If a Reportable Breach affects 600 individuals who are residents of Oregon, and 510 individuals who are residents of Washington, notice to media in both states is required.

If notice to media is required, it will be given without unreasonable delay, and in no event more than 60 calendar days after the date of discovery (as determined above). The content requirements for a notice to media are the same as the requirements for a notice to individuals. The Privacy Official is responsible for giving notice to media.