{COVERED ENTITY NAME}

NOTIFICATION TO AFFECTED INDIVIDUALS OF BREACH

|  |
| --- |
| Purpose: This Form is used to develop a policy and procedure for the health plan to notify individuals affected by a breach of protected health information. Retain this form in the health plan’s records for at least six (6) years from the date below. |

**SECTION A: Policy**.

It is the policy of the health plan that the plan will, upon discovering a breach of unsecured protected health information, report the breach to affected individuals (unless an exception applies). The plan will report the breach without unreasonable delay and in no case later than sixty (60) calendar days after the plan discovers the breach.

**SECTION B: Procedure**.

**1. Identification of Affected Individuals.** The Privacy Official will identify the number of individuals affected by a breach. The Privacy Official will maintain a log of affected individuals by using Form 11, Log of Individuals Affected by Breach. The Privacy Official will then gather the last known address of each affected individual using the plan’s records for that individual. If an individual has died, the Privacy Official will use the address of the individual’s next of kin or personal representative, if known. If the individual has specified (and not revoked) a preference to receive notification by electronic mail, the Privacy Official may send the notice by electronic mail.

**a. Insufficient or Out of Date Contact Information.** The plan’s contact information may be insufficient or out of date. This may prevent the plan from direct written (or email) contact to the affected individual. If so, and if ten (10) or more individuals have such insufficient or out of date information, the plan will: (i) place a conspicuous posting on the home page of the plan’s web site [Note: Delete (i) if the plan does not maintain a web site]; or (ii) place notice in major print or broadcast media, including media where the individuals affected by breach likely reside [Note: if (i) was deleted, renumber (ii) by deleting the phrase “(ii)”]. Such a notice in media or web posting will include a toll-free phone number (which must remain active for at least 90 days) where an individual can learn whether or not the individual’s unsecured protected health information was included in the breach.

The Privacy Official will determine which method ((i) or (ii), above), will be used. The Privacy Official will coordinate all necessary changes to the plan’s web site, if any. The Privacy Official will ensure that a toll-free phone number is established, if required. The Privacy Official may assign the responsibility for responding to inquires about the breach to a third party (such as a third party administrator). If the Privacy Official assigns such responsibility to a third party who is a business associate, the Privacy Official will update the relevant business associate agreement to ensure that the business associate treats the information as being subject to HIPAA.

**b. Urgency.** The Privacy Official may determine that there is urgency in disclosing the breach due to possible imminent misuse. If so, the Privacy Official may contact individuals by telephone in addition to, or in lieu of, the methods noted above.

**2. Notice to Affected Individuals.** The Privacy Official will use the attached letter to send to affected individuals to describe the breach. One notice may be addressed to both a plan participant and the participant's spouse and dependents who are affected by the breach, so long as: (a) they all reside at a single address; and (b) our notice clearly indicates on the notice the individuals to which the notice applies.

**[LETTER TO SEND TO INDIVIDUALS AFFECTED BY BREACH; RE-TYPE ON PLAN LETTERHEAD OR OTHERWISE INSERT PLAN CONTACT INFORMATION]**

[Insert name of individual affected by breach]

[Insert address]

Dear [Insert name of individual]:

The undersigned is the Privacy Official of the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [Insert plan name] (the “Plan”). The Plan is subject to the breach notification rules of the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”). HIPAA imposes certain restrictions on the Plan and how it maintains your protected health information (“PHI”). These restrictions include a requirement that the Plan generally protect the security of your PHI. If the Plan discovers a breach of the security of your PHI, the Plan is required to notify you of this breach.

The Plan recently discovered a breach of your PHI. This letter describes the details of this breach. The Plan takes this situation very seriously and is working to mitigate any harmful effect from this breach.

1. Overview. [Describe what happened, including the date of the breach and the date of the discovery of the breach, if known.]

2. Types of PHI. [Describe the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number or disability code)] \_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Steps to Protect Yourself. [Describe the steps the individual should take to protect himself or herself from potential harm resulting from the breach; e.g., using a credit monitoring service, especially if a Social Security number was included in the breached PHI] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. Plan’s Investigation. [Describe the Plan’s investigation of the breach, its efforts to mitigate losses and to protect against any further breaches]

5. Contact Procedures. Please contact the following to ask questions or learn additional information:

[Insert name or title of contact person]

[Insert toll-free phone number, email address, web site or postal address]

Again, we take this situation very seriously and are working diligently to resolve the situation. **[Note: This type of sentence is not legally required]** Please contact the above individual [Insert “office” if applicable] for more information.

Regards,

[Insert Privacy Official name]

QB\21427348.1