{COVERED ENTITY NAME}

BREACH IDENTIFICATION

Purpose: This Form is used to identify whether a breach has occurred under the HIPAA Breach Notification Rules. Retain this form in the health plan’s records for at least six (6) years from the date below.

**SECTION A: Identification of Unsecured Protected Health Information**

We previously identified the protected health information (“PHI”) we hold. We now must determine if this information is ever “unsecured.” PHI will be unsecured unless it is rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services (“HHS”).

Based upon our review of the PHI we hold, along with current HHS guidance, we conclude that we:

🞎 Always hold unsecured PHI, for example,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

🞎 Sometimes hold unsecured PHI; for example, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

🞎 Never hold unsecured PHI.

If the last box is checked (“Never hold unsecured PHI”), there is no need to complete the remainder of this Form 10.

**SECTION B: Verification of Holding of PHI**

The HIPAA breach provisions apply to a Breach of Unsecured PHI. The breach rule applies only if there is an acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted by the Privacy Rules, unless a risk assessment demonstrates that there is a low probability that the PHI has been "compromised." Verify if an exception applies such that these breach notification rules do not apply by completing Section C. Complete Section D to determine if the PHI was compromised. If we have doubt about the meaning of these terms in a particular situation, it is our policy to seek legal advice on the meaning of the unclear term.

**SECTION C: Exceptions to Breach Rules**

A “breach” excludes:

(1) Any unintentional acquisition, access, or use of PHI by the plan's workforce member or a person acting under the authority of the plan or the plan's business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rules.

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at our plan or our business associate to another person authorized to access PHI at our plan or our business associate (or an organized health care arrangement in which we participate) provided the information received as a result of such disclosure is not further used or disclosed in a manner not permitted by the Privacy Rules.

(iii) A disclosure of PHI where a covered entity or business associate 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.

**SECTION D: Compromised PHI**

The HIPAA Breach Notification Rule presumes that situations involving impermissible access, acquisition, use or disclosure of PHI is a breach. This presumption can be overcome if we demonstrate (or our business associate demonstrates to our satisfaction) that there is a low probability that the information has been compromised. This low probability is demonstrated by conducting a "risk assessment." Complete this Section D to perform our “risk assessment” of whether the PHI has been compromised.

A risk assessment must consider at least the following factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated. Describe these factors here:

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

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

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

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

These factors should be applied on a case-by-case basis for each individual whose PHI was potentially breached. The results could vary based upon individual factors. For example, suppose the PHI of two employees was improperly sent to a manager of a company. The manager supervises only one of the two employees; the other is in a separate division and the manager has no influence over the other individual. It is possible that the PHI would be compromised with respect to the employee who reports to the supervisor but not compromised with respect to the employee who works in the separate division.

Based upon these factors, we conclude as follows:

|  |  |  |
| --- | --- | --- |
| Name of Affected Individual | Low Probability PHI was Compromised? (Yes or No) | Comments on Risk Assessment |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

For individuals for whom we have concluded the PHI was compromised, list these individuals in *Form 11, Log of Individuals Affected by Breach*. Even if we conclude the PHI was not compromised, retain this *Form 10* so we can demonstrate our analysis.

**SECTION E: Notification of Breach**

We will use the definition of “Breach” and “Unsecured” PHI from above to determine if a Breach has occurred. We will also make reports as appropriate using *Form 13, Media Notice of Breach* and *Form 12, Notification to Affected Individuals of Breach*.

For these purposes, a Breach is “Discovered” as of the first day on which the Breach is known to us. We will know of a Breach if any person within our organization (including an employee, officer or agent of ours) knows of the Breach, other than the individual committing the Breach. A Breach is also “Discovered” if we should reasonably have known about the Breach.

Name of Security Official:

Signature:

Date:

QB\21427345.1