## Purpose

To set forth the procedures for responding to potential breaches of protected health information.

## Policy

This Policy applies only when there is a breach of a patient’s individually identifiable health information. A privacy or security breach occurs when there has been an acquisition, access, use, or disclosure of unsecured PHI that compromises the security or privacy of the information.

Under HIPAA and for purposes of this Policy, a breach does **not** include:

* An unintentional acquisition, access, or use of PHI by a workforce member or other person acting under the authority of the [COVERED ENTITY] or [COVERED ENTITY]’s Business Associate, if the acquisition, access, or use was made in good faith and within the scope of the workforce member’s authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.
* An inadvertent disclosure by a person who is authorized to access PHI at [COVERED ENTITY] or [COVERED ENTITY]’s Business Associate to another person authorized to access PHI at [COVERED ENTITY] or [COVERED ENTITY]’s Business Associate, or organized healthcare arrangement in which [COVERED ENTITY] participates, and information received as a result of such a disclosure is not further used or disclosed in a manner not permitted by the privacy rule.
* Disclosure of PHI where [COVERED ENTITY] or [COVERED ENTITY]’s 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 the information.

A breach is presumed to have occurred if there is an unauthorized access, acquisition, use, or disclosure of unsecured protected health information, *unless* [COVERED ENTITY] can demonstrate a low probability that the information was compromised. This determination must be based on a risk assessment of certain factors described in this Policy.

In the event a breach has occurred, [COVERED ENTITY] must notify the individuals whose information was breached and the Secretary of the U.S. Department of Health and Human Services, in accordance with the HIPAA breach notification rules and this Policy. In some cases, [COVERED ENTITY] may be required to notify the news media.

## Procedure

1. Reporting an Unauthorized Access, Use, or Disclosure of PHI.
   1. Any workforce member who learns that a potential breach of PHI may have occurred must immediately notify his or her supervisor and/or [COVERED ENTITY]’s Privacy Officer. If the potential breach relates to electronic information, the workforce member must also notify [COVERED ENTITY]’s Security Officer.
   2. Workforce members should report any suspected breach of unsecured PHI to the Privacy Officer as soon as possible, but in no case later than 48 hours after learning of the incident.
   3. The report of a potential breach should include the following information, to the extent available:
      1. A brief description of what happened, including the date of the potential breach and the date the suspected breach was discovered;
      2. Who used the PHI without appropriate permission or authorization and/or to whom the information was disclosed without permission or authorization;
      3. A description of the types of and amount of unsecured PHI involved in the breach;
      4. Whether the PHI was secured by encryption, destruction, or other means;
      5. Whether any intermediate steps were taken to mitigate an impermissible use or disclosure;
      6. Whether the PHI that was disclosed was returned prior to being accessed for an improper purpose; and
      7. If the PHI was provided to [COVERED ENTITY] under a Business Associate Agreement.
   4. Failure to report a suspected breach to the [COVERED ENTITY] may result in disciplinary action against employees, subcontractors, interns, or volunteers.
2. Investigating Potential Breaches of PHI. [COVERED ENTITY] must promptly investigate any security and/or privacy incident to determine whether there has been a breach of PHI. In making this determination, [COVERED ENTITY] shall consider the following:
   1. Whether the unauthorized or impermissible acquisition, access, use, or disclosure involved PHI.
   2. Whether [COVERED ENTITY] can demonstrate, based on the following factors, a low probability that the PHI has been compromised:
      1. The nature and extent of the information involved;
      2. The unauthorized person who used or received the information;
      3. Whether the information was actually acquired or viewed; and
      4. The extent to which the risk to the information has been mitigated.
   3. [COVERED ENTITY] must document the investigation and reasonable conclusions, including all facts relevant to the risk assessment. Documentation of findings and final actions from the investigation should be maintained as a part of [COVERED ENTITY]’s Privacy records and retained for six (6) years.
   4. If it is determined that a HIPPA violation has occurred, [COVERED ENTITY] must determine, in accordance with [COVERED ENTITY]’s Sanctions Policy, what disciplinary actions should be taken. The disciplinary action report documenting the violation should be placed in the staff’s personnel file.
3. Breach Notification Procedures. If [COVERED ENTITY] determines that a breach of unsecured PHI has occurred, [COVERED ENTITY] shall notify the affected individual(s), HHS, and the media (if required) in accordance with this Policy and the requirements of HIPAA’s breach notification rules. Any notice provided pursuant to this Policy must be approved and directed by [COVERED ENTITY]’s Privacy Officer. No other personnel may, absent express authorization of the [COVERED ENTITY]’s Privacy Officer, provide the notice required by this Policy.
   1. Notice to Individuals. When a breach of PHI has occurred, the [COVERED ENTITY] shall notify the affected individual(s) without unreasonable delay and in no case later than 60 days after the breach is discovered.
      1. *Contents of Notice*. The notice must be in writing and written in plain language, and must include, to the extent possible:
         1. A brief description of the incident (e.g., the date of the breach and the date it was discovered);
         2. A description of the types of information involved (e.g., whether the breach involved names, social security numbers, birthdates, addresses, diagnoses, etc.);
         3. Any steps the affected individual(s) should take to protect him or herself from potential harm resulting from the breach;
         4. A brief description of what [COVERED ENTITY] is doing to investigate, mitigate, and protect against further harm or breaches; and
         5. Contact information for [COVERED ENTITY] (or business associate, as applicable) (e.g., toll-free telephone number, e-mail address, website, or postal address).
      2. *Method of Notification*. The [COVERED ENTITY] shall notify the affected individual by first class mail to the individual’s last known address. Notice may be sent via e-mail if the patient has agreed to accept notification via electronic means.
      3. *Substitute Notice*. If [COVERED ENTITY] has insufficient or out-of-date contact information that precludes written notification to the individual, the [COVERED ENTITY] shall provide a substitute form of notice that is reasonably calculated to reach the individual.
         1. Fewer than 10 individuals: Where there is insufficient or out-of-date contact information for fewer than 10 individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.
         2. 10 or More Individuals: Where there is insufficient or out-of-date contact information for 10 or more individuals, substitute notice shall:
            1. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
            2. Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
      4. *Urgent Situations*. In any case deemed by [COVERED ENTITY] to require urgency because of possible imminent misuse of unsecured PHI, [COVERED ENTITY] may provide information to individuals by telephone or other means, as appropriate, in addition to the required written notice.
      5. *Deceased Individuals*. If [COVERED ENTITY] has the address of the next of kin or personal representative of the deceased individual, it may provide written notification by first-class mail to either the next of kin or personal representative.
   2. Notice to HHS. If [COVERED ENTITY] determines that a breach of protected health information has occurred, [COVERED ENTITY] shall also notify HHS of the breach as follows:
      1. 500 or More Affected Individuals. For breaches of unsecured PHI involving 500 or more individuals, [COVERED ENTITY] must notify HHS of the breach contemporaneously with the notice to the individuals and in the manner specified on the HHS website.
      2. Fewer than 500 Affected Individuals. For breaches of unsecured protected health information involving fewer than 500 individuals, [COVERED ENTITY] may report the breach immediately to HHS in the manner specified on the HHS website. If the Privacy Officer does not immediately report the breach to HHS, s/he shall maintain a log or other documentation of such breach and, not later than 60 days after the end of each calendar year, provide the notification to HHS in the manner specified on the HHS website.
   3. Notice to Media. For a breach of unsecured protected health information involving more than 500 residents of a particular state or jurisdiction, [COVERED ENTITY] shall, following the discovery of the breach, notify prominent media outlets serving the state or jurisdiction. The notification must be made without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The notification must contain the information required for individual notices as described in Section 3.a.i above.
4. No Retaliation. [COVERED ENTITY] maintains an open-door policy regarding compliance with HIPAA. Employees, subcontractors, interns, and volunteers are encouraged to speak with the Privacy/Security Officer or other appropriate individual regarding any concerns they may have with [COVERED ENTITY]’s HIPAA compliance program or initiatives designed to maintain and enhance privacy and security controls. Neither [COVERED ENTITY] nor anyone affiliated with [COVERED ENTITY] may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising any right established by, or for participating in any process provided for by, these policies or the law, including:
   1. Filing a complaint with [COVERED ENTITY];
   2. Filing a complaint with governmental authorities;
   3. Assisting or participating in an investigation or compliance review by [COVERED ENTITY] or its agents;
   4. Testifying in a proceeding or hearing by governmental authorities under HIPAA; or
   5. Opposing any act or practice made unlawful by HIPAA, provided the individual has a good faith belief that the practice opposed is unlawful and the manner of opposition is reasonable and does not involve an impermissible disclosure of PHI.

Any individual who believes that a form of retaliation or intimidation is occurring or has occurred should report the incident to the [COVERED ENTITY]. The [COVERED ENTITY] should treat such a report as a complaint and investigate it accordingly

**HIPAA PRIVACY BREACH LOG**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date of Breach** | **Date of Discovery** | **Description of Incident** | **# of Individuals Affected** | **Notifications Made (method, media used, dates, etc.)** | **Notes** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

This log will be submitted to the Secretary of the Department of Health and Human Services within 60 days after the year end. Refer to <http://www.hhs.gov> for how to submit this breach notification.

**HIPAA BREACH ANALYSIS TOOL**

**Name of person completing form: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date incident occurred: \_\_\_\_\_/\_\_\_/\_\_\_\_\_ Date incident discovered: \_\_\_\_\_/\_\_\_/\_\_\_\_\_**

**Brief description of incident (including number of individuals affected): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**1. Was protected health information (“PHI”) involved?** (PHI is any individually identifiable information, including demographic information, that is created or received by a healthcare provider and that 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).

\_\_\_\_ Yes (continue to Question 2)

\_\_\_\_ No (no breach reporting required under HIPAA)

Describe the information involved: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

2. **Was the PHI unsecured?** (“Unsecured” PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in HHS guidance, which can be found at

[www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html](http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html).)

\_\_\_\_ Yes (continue to Question 3)

\_\_\_\_ No (no breach reporting required under HIPAA)

Describe the PHI (e.g., whether it was verbal/oral, paper, or electronic; if electronic, whether it was encrypted, password-protected, etc.) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

3. **Was the PHI acquired, accessed, used, or disclosed in a manner not permitted by the HIPAA Privacy Rule?** (A violation of the “minimum necessary” standard is not permitted by the Privacy Rule. On the other hand, a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and that occurs despite reasonable safeguards and proper minimum necessary procedures is not a violation of the Privacy Rule. You may wish to consult legal counsel to determine if the acquisition, access, use or disclosure was permitted by the Privacy Rule).

\_\_\_\_ Yes (continue to Question 4)

\_\_\_\_ No (no breach reporting required under HIPAA)

Describe who acquired, accessed, used, and/or disclosed the PHI; whether the person(s) was authorized or unauthorized; and how the PHI was acquired, accessed, used, or disclosed: \_\_\_\_\_\_\_\_

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

**4.** **Does an exception apply?** (Check any that applies)

* **Exception A** - A breach does not include any unintentional acquisition, access, or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate, if it: was made in good faith; and as within the course and scope of authority; and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.
* **Exception B** - A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.
* **Exception C** - A breach does not include disclosure of PHI where the covered entity or business associate has a good faith belief that the unauthorized person who received it would not reasonably have been able to retain the information. These incidents would not constitute reportable breaches.

\_\_\_\_ Yes (no breach reporting required under HIPAA)

\_\_\_\_ No (Continue to Question 5)

**5.** **Risk Assessment.** An acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach and must be reported unless the covered entity can demonstrate a low probability that the PHI has been compromised. This determination must be based on a risk assessment of least the following 4 factors:

**Factor 1** – Nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. (Consider whether sensitive financial information, e.g., credit card numbers or social security numbers, was involved, or whether sensitive clinical information was involved, e.g., information related to mental health or sexually transmitted diseases, as well asl the amount of detailed clinical information involved, e.g., diagnosis, medication, medical history, test results, etc. Consider whether the PHI could be used in a manner adverse to the patient or to further the unauthorized recipient’s own interests).

Describe the PHI involved, including the types of identifiers and the likelihood of re-identification \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

* Supports reporting
* Does not support reporting

**Factor 2** – The unauthorized recipient or user of the PHI. This factor must be considered even if the impermissible acquisition, use, or disclosure was purely internal. Consider whether the unauthorized person is also a covered entity subject to HIPAA requirements or a government employee or other person required to comply with other privacy laws.

Describe who used or received the PHI and whether s/he has any legal or ethical obligation to protect the PHI \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

* Supports reporting
* Does not support reporting

**Factor 3** – Whether the PHI was actually acquired or viewed (if ePHI is involved, this may require a forensic analysis of the computer or device to determine if the information was accessed, viewed, acquired, transferred, or otherwise compromised).

Describe whether the PHI was actually acquired or viewed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

* Supports reporting
* Does not support reporting

**Factor 4** – The extent to which the risk to the PHI has been mitigated (e.g., did you obtain satisfactory assurances from the recipient, in the form of a confidentiality agreement or similar means, that he or she will not further use or disclose, or has completely returned or has or will completely destroy, the PHI?

Describe the mitigation steps taken \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

* Supports reporting
* Does not support reporting

**Factor 5** – Any other relevant factors (indicate “none” if appropriate) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

* Supports reporting
* Does not support reporting

Based on the above factors, is there a low probability that the PHI has been compromised?

\_\_\_\_ Yes (no breach reporting required under HIPAA)

\_\_\_\_ No (breach reporting is required under HIPAA)

Signature of person completing this form: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_