HIPAA Breach/Risk Assessment Worksheet

Breach notification is required when (1) there has been a use/disclosure of protected health information (PHI) in violation of 45 CFR Subpart E, and (2) the covered entity/business associate cannot demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment (45 CFR 164.402).

Section 1 – Basic breach test

If the answer to any of the questions in section 1 is “No” then -
- There is no breach
- Stop the analysis, notification is not required
- Document the case and provide appropriate training to the individuals involved

<table>
<thead>
<tr>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  ☐  ☐ Did the use/disclosure violate the privacy rule? (e.g. more than the minimum necessary; information was PHI; sent to unauthorized party; etc.)

  ☐  ☐ Did this use/disclosure involve unsecured PHI (not rendered unusable, unreadable, indecipherable)?

If the answer to all of the above questions in this section is “Yes”, continue to section 2...

Section 2 – Does an exception apply?

If the answer to any of the questions in section 2 is “Yes” then –
- There is an exclusion
- Stop the analysis, notification is not required
- Document the case and provide appropriate training to the individuals involved

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  ☐  ☐ Was this an unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a CE or a BA, and was such acquisition, access, or use made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted?

  ☐  ☐ Was this an inadvertent disclosure by a person who is authorized to access PHI at a CE/BA to another person authorized to access PHI at the same CE/BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.

  ☐  ☐ Is there a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information?

If the answer to each of the above questions in this section is “No”, proceed to section 3...

Section 3 – Is there a low probability that the PHI has been compromised?

Barring the exceptions in section 2 above, an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
(iii) Whether the protected health information was actually acquired or viewed; and
(iv) The extent to which the risk to the protected health information has been mitigated.

These four factors along with any other factors relevant to the particular scenario should be taken together to determine if it can be demonstrated that the probability of compromise is low.
### HIPAA Breach/Risk Assessment Worksheet

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Can it be demonstrated that there is a low probability that the PHI has been compromised based on the 4 factor risk assessment taken together with any other relevant factors?

If the answer to the above question is “No”, then:
- Notification is required. For detailed requirements, see 45 CFR Subpart D: 164.404 Notification to individuals; 164.406 Notification to the media; 164.408 Notification to the Secretary, and 164.410 Notification by a business associate.
- Document the case and provide appropriate training to the individuals involved.

### Section 4 – Information of person completing the form

<table>
<thead>
<tr>
<th>Name:</th>
<th>Title:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Signature:</th>
<th>Date:</th>
</tr>
</thead>
</table>