# HIPAA Four-Factor Risk Assessment

The HIPAA Breach Notification Rule requires consideration of at least four factors by completing a risk assessment after discovering a breach of unsecured protected health information. Rather than determine the risk of harm, the risk assessment determines the probability that PHI has been compromised based on four factors.

The following was reported to CBCIH as a possible breach of PHI:

**Agency Name**: ________________________________________

**Type of Breach**:________________________________________

**Date of Breach**:_________________

Note: Refer to the completed *CBCIH Data Breach Reporting Form 100A* for details.

1. **Describe the nature and extent of the PHI involved, including the types of identifiers, and the likelihood of re-identification.**
   *Describe:*

*<u>Example:</u> Social Security Number, credit cards, financial data, diagnosis, treatment, medications*, *behavioral health, substance abuse, and/or sexually transmitted diseases of patient(s).*

**2. Identification of the unauthorized person(s) who used the PHI or to whom the PHI was disclosed.**

**a) Does the person have obligations to protect privacy and security?** ☐ **Yes** ☐ **No**

*<u>Example:</u> is the person a covered entity required to comply with HIPAA, or a government employee, or other person who is required to comply with other privacy laws?*

**b) Does the person have the ability to re-identify the PHI?** ☐ **Yes** ☐ **No**

*Describe who used or received the PHI, whether they have legal obligation to protect the PHI, and whether they can re-identify the PHI (if the PHI is de-identified):*

*Describe:*

**3. Determine whether the PHI was actually viewed or accessed.** Consider whether the PHI was actually acquired or viewed. (If electronic PHI is involved, this may require a forensic analysis of the computer to determine if the information was accessed, viewed, acquired, transferred, or otherwise compromised. Attach report from a computer forensic analyst, if one was obtained.)

a) **Was the PHI actually acquired or viewed?** ☐ **Yes** ☐ **No**

**4. Determine the extent to which the risk to the PHI has been mitigated.** *Providers should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.*

a) **Can the person who received the PHI provide satisfactory assurances that the PHI will not be further used or disclosed, or that it will be destroyed?** ☐ **Yes** ☐ **No**
*Example:* ***T**hrough a confidentiality agreement or similar means*.

b) **What level of effort has been expended to prevent future related issues and/or to lessen the harm of the actual breach? (e.g., training, policies and procedures, etc.)**

*Describe risk mitigation steps taken:*

*Describe any other relevant factors:*

*These factors should be considered in combination and not in isolation when conducting a risk assessment. If an entity has an incident and its risk assessment concludes that there was a very low probability that the PHI was compromised, it may choose to not notify the affected individuals or the Department of Health and Human Services Office for Civil Rights (OCR). However, the Final Omnibus Rule requires that the entity maintain a "burden of proof" if its conclusions are called into question. If the OCR investigated the covered entity, it would be required to provide conclusive documentation of its incident risk assessment and analysis as to why the incident did not result in a "compromise" of PHI. If the entity doesn't meet that burden of proof, it could be found to have been negligent in not notifying the affected individuals and subject to substantial fines, penalties, and corrective action.*

## Four Factor Risk Assessment Conclusion

The Final Omnibus Rule requires that the entity maintain a burden of proof if its conclusions are called into question. During an investigation the OCR would require conclusive documentation as to why the incident did not result in a compromise of PHI. If the entity doesn't meet the burden of proof, it could be found to have been negligent is not notifying the affected individuals and subject to fines, penalties and/or corrective action.

**Based on the results of the Four Factor Risk Assessment, is there a low probability that the PHI has been compromised?**

☐ Option 1: No, there is not a low probability; there is a high probability**.**
****Breach reporting is required under HIPAA.**

☐ Option 2: There is a low probability. *No breach reporting required under HIPAA.*
****You should still keep this record or document why this incident did not result in a compromise of PHI.**

Person completing this form:

**Signature:** ____________________________

**Name:** ____________________________

**Title:** ____________________________

**Date:** _______________