

# RISK OF HARM ASSESSMENT

## A COPY OF THIS ASSESSMENT MUST BE SUBMITTED WITH THE POST INCIDENT REPORT

### STEP 1: Review for exclusions:

1. Was the data encrypted? If PHI was compromised, was it encrypted per DHHS Guidance 74 FR 19006 (2009)? *See*, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>.  
 Yes     No
2. Was the unintentional acquisition, access or use of PII (or PHI) made in good faith and within the scope of authority of an individual or entity, for lawful purposes of the individual or entity, by a person or business associate, and is not subject to further unauthorized use or disclosure?  
 Yes     No
3. HIPAA Only: Was the PHI inadvertently disclosed by a person who is authorized to access PHI at a HIPAA covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure was not further used or disclosed in an unauthorized manner?  
 Yes     No
4. HIPAA Only: Does the HIPAA covered entity or business associate have a good faith belief that the unauthorized person to whom the disclosure of PHI was made would not reasonably have been able to retain such information?  
 Yes     No

If any of the above exclusions apply and you answered “Yes” to any of the questions above, there is no breach and notification is not required. Document the decision.

# RISK OF HARM ASSESSMENT

**STEP 2:** If there are no exclusions, the Department should complete the following risk assessment to analyze possible risks to affected individuals as a result of the Unauthorized Disclosure and as a guide to assist with the final decision-making regarding requirements for breach notification to impacted individuals.

| RISK ASSESSMENT FACTORS  | HIGH RISK OF COMPROMISE (2 POINTS)  | MEDIUM TO LOW RISK OF COMPROMISE (1 POINT)   | NO IMPACT (0 POINTS)  | RATING SCORE |
|--|---|--|---|--------------|
| <b>The nature and extent of the PII<sup>1</sup> used or disclosed</b>  | <p>Unauthorized use or disclosure of electronic PII (W. Va. Code § 46A-2A-101 - An individual's first name or first initial and last name in combination with SSN, driver's license/State ID card, financial account numbers).</p> <p>Unauthorized use or disclosure of unsecured Protected Health Information (PHI).</p> | Unauthorized use or disclosure of electronic PII associated with an individual (Excludes PHI).   | Unauthorized use or disclosure with no sensitive PII.   |              |
| <b>The unauthorized recipient of the use or disclosure (or who illegally obtained the PII).</b>                        | <p>Untrusted/Unknown recipient.<br/>Lost or stolen.</p>   | Trustworthy recipient- for example, an individual with contractual obligations to the department, or has confidentiality obligations – such as an attorney or medical professional.      | Trusted recipient - for example, a member of the workforce.   |              |
| <b>Disposition of Unauthorized Use or Disclosure. Assess what happened after the initial use or disclosure of PII?</b> | <p>PII was acquired.<br/>Cyber Incident.<br/>Obtained for personal gain/malicious harm.</p>   | PII was viewed/or partially viewed but not acquired.   | PII was not viewed or acquired.   |              |
| <b>The extent to which the risk to the PII has been mitigated.</b>   | <p>No mitigation.<br/>Unable to retrieve PII.<br/>Unsure of disposition or location.<br/>PII is pending re-disclosure or already re-disclosed.<br/>No security controls.<br/>Security controls such as password or encryption were compromised.</p>   | <p>We have good-faith reason to believe that the PII has not and will not be used or disclosed.<br/>PII destroyed, but not confirmed.<br/>Electronically deleted, but not confirmed.</p> | <p>We have good-faith reason to believe that the PII has not and will not be used, disclosed, or retained.<br/>Data wiped.<br/>Information/device meets security control standards.</p> |              |
| <b>Any other factors or information which can assist in determining whether the PII was compromised:</b>               |   |  |   |              |

<sup>1</sup> PII is the umbrella term for all personally identifiable information. PII includes all categories of sensitive information including Protected Health Information (PHI). If other categories of sensitive PII have been compromised that have more restrictive breach notification requirements, they must be followed.

# RISK OF HARM ASSESSMENT

**STEP 3.** Based upon on the total factor rating points, the incident is categorized into one of three levels as follows:

- Total score of 7 or 8 = High Risk: PII has been compromised.
- Total score of 5 or 6 = Medium Risk: PII may have been compromised.
- Total score of 4 or less = Low Risk or No Impact: There is likely a low risk of compromise or no impact.

**STEP 4:** Determine if notification is required based upon your risk assessment and risk ratings.

**Note: If time permits, forward a draft copy of individual notification to BRIM for review and assistance.**

A. Examples for where notification is not required:

- A laptop is lost/stolen, then recovered and forensic analysis shows the PII was not accessed, altered, transferred or otherwise compromised.
- An envelope, email, or file (containing PII) was returned, electronically deleted or properly destroyed.

**Note: Advance BRIM approval is needed if notice is not required, but the Department determines it is appropriate.**

B. Examples for where notification is required:

- There was an unauthorized disclosure of PHI to a third party. The unsecured/unredacted electronic data contained patient names, patient addresses and diagnosis information.
- An unknown recipient with access to the encryption key acquired encrypted information (first name, last name, SSN, and driver's license number).
- A workforce member who is using their own mobile device, for work related purposes, reports it lost or possibly stolen. The device had documents containing PII. The device was not password protected and the security officer is not able to wipe any data from the device.