# RISK OF COMPROMISE ASSESSMENT

**A COPY OF THIS ASSESSMENT MUST BE SUBMITTED WITH THE POST INCIDENT RESPONSE ASSESSMENT**

DEPARTMENT/AGENCY: _____ OT INCIDENT NUMBER: _____ INCIDENT RESPONSE LEAD:_____

**STEP 1**: Review for exclusions:

1. Was the data containing Personally Identifiable Information (PII) [1] encrypted? (If PHI was compromised, was it encrypted per DHHS Guidance 74 FR 19006 (2009)? *See*, 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

## FOR HIPAA IMPACTED AGENCIES ONLY

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 to the impacted individual(s) is not required. Document the decision in your file and provide a copy to the State Privacy Office.

[1] 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. PHI is regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), and any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The US Dept. of Health and Human Resources (DHHS) through the Office for Civil Rights (OCR) enforces regulations set forth through HIPAA.

# RISK OF COMPROMISE ASSESSMENT

**STEP 2:** If there are no exclusions, 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 |
|---|---|---|---|---|
| **The nature and extent of the PII used or disclosed** | • 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, or financial account numbers).<br>• Unauthorized use or disclosure of unsecured PHI. | Unauthorized use or disclosure of electronic PII associated with an individual (Excludes PHI). | Unauthorized use or disclosure with no sensitive PII. | |
| **The unauthorized recipient of the use or disclosure (or who illegally obtained the PII).** | • Untrusted/Unknown recipient.<br>• Malicious actor or insider. | Trustworthy recipient - for example, an individual with contractual obligations to the department. | Trusted recipient - for example, a member of the workforce, an attorney, medical professional, US Post Office, or other government agency. | |
| **Disposition of Unauthorized Use or Disclosure. Assess what happened after the initial use or disclosure of PII.** | • PII was acquired<br>• Cyber incident.<br>• Obtained for personal gain/malicious harm. | PII was viewed/or partially viewed but not acquired. | PII was not viewed or acquired. | |
| **The extent to which the risk to the PII has been mitigated.**[2] | • 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 or compromised security controls (such as access control or encryption). | • Department has good-faith reason to believe that the PII has not and will not be used, disclosed, or retained.<br>• PII physically or electronically destroyed, but not confirmed.<br>• Security controls policy applies, but cannot be confirmed. | • Department has good-faith reason to believe, through **credible written assurance**, that the PII has not and will not be used, disclosed, or retained.<br>• Data wiped remotely.<br>• Security controls policy applies and confirmed through validation. | |

**TOTAL POINTS: _____**

**Any other factors or information which can assist in determining whether the PII was compromised:**

[2] Mitigation is reducing the impact of risk. Examples include: Steps to limit further damage by shutting down affected hardware, breach notification, terminating access if workforce member is inappropriately accessing confidential data or PHI, etc.

# RISK OF COMPROMISE ASSESSMENT

**STEP 3**. Based 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 to the individual is required based upon your risk assessment and risk ratings.
**Note: Prior to sending any notification, obtain approval from BRIM. This does not apply in cases of Federal Tax Information, with notifications required within 24 hours.** A draft copy of any notification must be sent to the Board of Risk and Insurance Management (BRIM) for review.

A. Examples 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, and there is evidence that the envelope, email or file was not accessed, altered, transferred or otherwise compromised.

B. Examples 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 without authorized access to the encryption key acquired encrypted information (first name, last name, SSN, and driver's license number).
- A workforce member who is using his 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.

*****Place this ROCA in your file and submit a copy to all required parties with the Post Incident Response Assessment. *****