

 **POST INCIDENT RESPONSE ASSESSMENT**

**This report must be provided to the parties listed on the last page within 30 calendar days of filing the initial Incident Report**

The Privacy Incident Response Assessment (PIRA) contains pre-decisional, confidential information, including internal risk assessments, and constitutes internal memoranda exempt from the Freedom of Information Act, W. Va. Code 29-B-1 et seq. The PIRA and the information contained herein shall only be disclosed to the extent necessary in the deliberative process or as required by law.

**SECTION 1 – INCIDENT REPORTING CONTACT INFORMATION**

Department/Agency/Division:

|  |
| --- |
|  |

Name (of person who reported the incident):

|  |
| --- |
|  |

Phone Number:

|  |
| --- |
|  |

Email:

|  |
| --- |
|  |

Department Privacy Officer:

|  |
| --- |
|  |

Agency/Division Privacy Officer (if applicable):

|  |
| --- |
|  |

Office of Technology (OT) Incident Tracking Number:

|  |
| --- |
|  |

**SECTION 2 – INCIDENT INFORMATION**

2.1 Date incident occurred or timeframe during which the incident occurred:

|  |
| --- |
|  |

2.2 Date of initial incident report:

|  |
| --- |
|  |

2.3 Physical location of incident:

|  |
| --- |
|  |

2.4 How was incident reported?

|  |
| --- |
|[ ]  Office of Technology Online Security & Privacy Incident Reporting System |
|[ ]  Other (Please Specify): |
|  | Click here to enter text. |

2.5 How was the incident discovered?

|  |
| --- |
|  |

2.6 Brief description of the incident and any action taken at time of discovery to contain or minimize its impact:

|  |
| --- |
|  |

2.7 Was the data containing Personally Identifiable Information (PII) encrypted1, rendering the data elements unusable, unreadable or indecipherable? If PHI was compromised, was it encrypted per DHS Guidance 74 FR 19006 (2009)? **(*See,*** [**https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html**](https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html)**).** If “Yes”, 2.8 is also “Yes.”

|  |  |
| --- | --- |
|[ ]  Yes |[ ]  No  |

1 Encrypted, in this context, means there is a low probability of assigning meaning without the use of a confidential process or key, and that process or key is not available to any unauthorized person in possession of the PII.

2.8 Has it been determined by the Department Privacy Officer that the incident is only an event that has been now resolved?

|  |  |  |
| --- | --- | --- |
|[ ]  Yes |[ ]  No  | **DPO Initials: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

**IF YES, STOP HERE. THE DEPARTMENT PRIVACY OFFICER WILL INITIAL AND SUBMIT TO THE PARTIES LISTED ON LAST PAGE. YOU DO NOT NEED TO COMPLETE THE REST OF THE FORM.**

2.9 Was the incident the result of policies not being followed? (Consider your agency, department, and Executive Branch policies & procedures.)

|  |  |
| --- | --- |
|[ ]  Yes |[ ]  No |

If Yes, indicate by name and number:

|  |
| --- |
|  |

2.10 When was policy/procedure training last presented to the employee(s) involved in the incident?

|  |  |
| --- | --- |
| **Date:** |  |

2.11 Provide the names of the individuals who participated in managing the incident response:

|  |
| --- |
| Click here to enter text. |

2.12 Type of Incident:

|  |  |
| --- | --- |
|[ ]  Internal Unauthorized Disclosure |[ ]  External Unauthorized Disclosure |
|[ ]  Other (Please specify if Loss/Theft, SSA, IRS etc.): |
|  |  |

2.13 List **types** of PII (including PHI) that were disclosed. **>>DO NOT LIST ACTUAL PII<<**

|  |
| --- |
|  |

2.14 Provide the number of individuals affected or potentially affected:

|  |
| --- |
|  |

2.15 If a privacy complaint was filed by an individual who alleges their PII was inappropriately accessed or disclosed, did the complainant receive a response from the department?

|  |
| --- |
|[ ]  N/A (No privacy complaint was made) |
|[ ]  Yes |
|[ ]  No (Please explain): |
|  |  |

**SECTION 3 – SUMMARY OF RISK OF HARM / COMPROMISE ASSESSMENT**

*Note: You must attach the completed Risk of Harm / Compromise Assessment available on the State Privacy Office website (*[*http://www.privacy.wv.gov/incidentresponse*](http://privacy.wv.gov/incidentresponse/Pages/default.aspx)*).*

**For HIPAA (only):**

3.1 An exclusion applies to the unsecured PHI (Step 1 of the Risk of Compromise Assessment).

|  |  |
| --- | --- |
|[ ]  Yes |[ ]  No |

|  |  |  |  |
| --- | --- | --- | --- |
| 3.2 The level of compromise is (Step 2): | [ ]  | No Impact or Low Risk |[ ]  Medium to High Risk |

**For Non-HIPAA (only):**

3.3 Did this incident meet the criteria of a potential breach (Step 2 of the Risk of Harm Assessment).

|  |  |
| --- | --- |
|[ ]  Yes |[ ]  No |

|  |  |  |
| --- | --- | --- |
| 3.4 The level of harm is (Step 3): |[ ]   No Impact or Low to Medium Risk  |[ ]   High Risk |

**SECTION 4 – NOTIFICATION TO INDIVIDUALS**

4.1 Indicate the status of notification for this incident.

1. **Notification is not required:**

|  |
| --- |
|[ ]  HIPAA: Due to a low risk of compromise or no impact, notification is not being made. Do not complete questions 4.2-4.5. Skip to Section 5. |
|[ ]  Non-HIPAA (W. Va. Code § 46A-2A-101): Due to a low or medium risk of harm or no impact, notification is not being made. Do not complete questions 4.2-4.5. Skip to Section 5. |

1. **Notification is required and was already issued due to time constraints:**

|  |
| --- |
|[ ]  Special Notification (SSA, PCI, FTI, etc.): Due to compliance with industry laws (other than W. Va. Code § 46A-2A-101) notification is being made. |
|  | Specify Law: |  |
|  | Date of Notification: |  |

1. **Notification is mandated or appropriate; and approval for notification is being requested** (Each of these circumstances requires approval from BRIM prior to notification.)**:**

|  |
| --- |
|[ ]  HIPAA: Due to a medium or high risk of compromise, notification is required by HIPAA and HITECH Act. Provide any additional details necessary in box below. |
|[ ]  Non-HIPAA: Due to a high risk of compromise, notification is required by WV Breach Law (W. Va. Code § 46A-2A-101). Provide any additional details necessary in box below. |
|[ ]  Notification is not mandated by law, but appropriate for the circumstances. In the box below, provide a detailed description of why notification should be made. |
|  |

**4.2 Approval for notification to individual(s) or OCR:**

1. NOTIFICATION TO INDIVIDUALS OR OCR MUST BE APPROVED IN ADVANCE BY BRIM, unless time-frame does not permit BRIM approval due to other regulations (e.g. Federal Tax Information regulations)
2. To receive approval, submit a thorough *draft* of this form (completed through Section 5.2, except for 4.3); the ROCA or ROHA; and, a *draft* of the notification, to lori.l.tarr@wv.gov; and, sue.c.haga@wv.gov.
3. After approval of the notification is received and the notifications are issued, submit the final PIRA, ROCA or ROHA, and a copy of the notification to the parties listed in Section 5.

1. If the time-frame for notification does not allow for approval by BRIM, submit the final PIRA, ROCA or ROHA, and a copy of the notification within three business days after notifications are issued.

4.3 Indicate the format of the notifications (Final PIRA only – post notification):

|  |
| --- |
|[ ]  Letter |
|[ ]  Email |
|[ ]  If other method(s) used, please indicate: |
|  |  |
|  Date Sent: |  |

**SECTION 5 – INCIDENT OUTCOME**

5.1 What was the outcome of the incident? (Be specific and include actions taken to resolve and/or mitigate the incident.) **NOTE: If a police report was filed, please attach a redacted copy.**

|  |
| --- |
|  |

5.2 What measures have been, or will be, implemented to prevent this type of incident from reoccurring?

(Check all that apply.)

|  |
| --- |
|[ ]  Additional Training |
|[ ]  Departmental Policy or Procedure Change – Security  |
|[ ]  Departmental Policy or Procedure Change – Privacy  |
|[ ]  System Change |
|[ ]  Improved Monitoring |
|[ ]  Physical Security Change |
|[ ]  Other (Please specify): |
|  |  |

**THE DEPARTMENT PRIVACY OFFICER MUST PROVIDE COPIES OF THIS REPORT TO:**

* **State Privacy Office**
* **Office of Technology – Chief Technology Officer & Chief Information Security Officer**
* **Cabinet Secretary**
* **Director of the Board of Risk and Insurance Management (BRIM)**
* **Others as applicable**

**SECTION 6 – To be completed by the State Privacy Office**

6.1 Was a Privacy Board convened?

|  |  |
| --- | --- |
|[ ]  Yes (indicate date): |  |
|[ ]  No |  |

6.2 Is notice to the Secretary of the US Department of Health and Human Services required?

|  |  |
| --- | --- |
|[ ]  Yes (indicate date): |  |
|[ ]  No |  |

6.3 Date this report was received in State Privacy Office (stamp date):

|  |
| --- |
|  |

6.4 State Privacy Office Incident Tracking Number:

|  |
| --- |
|  |