POST INCIDENT RESPONSE ASSESSMENT

This report must be provided to the parties listed in Section 6 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 REPORT INFORMATION

SPO Tracking Number: _____ OT Tracking Number: _____

Date of initial incident report: _____

Department: _____

Bureau/Division: _____

Agency/Office: _____

Name (of person who reported the incident): _____

Phone Number: _____

Email: _____

Department Privacy Officer: _____

Agency Privacy Officer (if applicable): _____

1.1 How was incident reported?

☐ Office of Technology Online Security & Privacy Incident Reporting System
☐ Other (Please specify below):

_____

1.2 Was this incident reported to law enforcement?

If yes, attach a copy of the report. If the report is not available, identify the law enforcement agencies to which a report was made. (Mark all that apply.) ○ Yes ○ No

☐	Local (Municipal or County)	Enter date of report here:	
☐	State Police	Enter date of report here:	
☐	Federal	Enter date of report here:	

Provide the ID number of report, identify the law enforcement agency below.

_____

SECTION 2 – INCIDENT INFORMATION

2.1 Date incident occurred or began:

2.2 Date incident ended (if applicable):

2.3 Date range for incident if specific dates are unknown:

2.4 Date incident was detected:

2.5 Physical location of incident:

2.6 How was the incident or suspected incident discovered?

2.7 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):

⚠ **Attention: Event Classification or Incident Withdraw Determination**

This section is to determine and document whether a reported incident qualifies as either (1) an **event**, or (2) can be **withdrawn**. To withdraw an incident, it must be *previously approved* by the State Privacy Office in writing.

If you know that this incident does not qualify either as an event, or for withdraw, skip to Question 2.13 – Incident Elements.

Event Classification - Answer Questions 2.8 – 2.10, and 2.12.

2.8 Encryption status:

1. Does this incident involve an email that was sent *unencrypted* outside of the wv.gov network, or otherwise against to policy? If yes, proceed to Question 2.13.	-Select-
2. **Non-HIPAA only:** Was the data containing Personally Identifiable Information (PII) encrypted[1], rendering the data elements unusable, unreadable or indecipherable?	-Select-
3. **HIPAA only:** Was the data containing Protected Health Information (PHI) encrypted per NIST standards or an encryption process equally effective to the NIST standard?[1,2]	-Select-

Notes:

- [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] To determine if the encryption meets the NIST standards, (*See,* https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html).
- If 2.8.1 or 2.8.2 is “Yes”, then in 2.12 check "Yes", initial and submit according to instructions in Section 6.

2.9 Classification determination when encryption is not a relevant to the incident:

1. Was PII accessible by an unauthorized individual?	-Select-
2. Was PII disclosed to an unauthorized individual?	-Select-
3. Was PII used, modified, or destroyed in an unauthorized manner?	-Select-

If the answer to *each* of the questions in 2.9 is “No”, this incident *could* be classified as an event; however, the incident must also be fully resolved.

2.10 For incidents where encryption status is not a factor, describe the following:

1. Circumstances, including other controls, that kept the data containing PII from unauthorized access, disclosure or use (e.g. returned fully sealed, never unopened envelope; pseudonymization); and
2. How the incident was fully resolved.

2.11 Withdraw Documentation: Have you received approval to withdraw this incident from the State Privacy Office? If so, click the "Yes" box, select the appropriate reason for the withdraw, and describe fully in the text box below. ☐ Yes

◯	1. The individual whose PII was involved is responsible for causing the incident.
◯	2. An external organization outside the State of West Virginia is responsible for the incident[1]
◯	3. The reported incident was determined not to be privacy or security related, or was otherwise errantly reported.[2]
◯	4. The reported incident only involved publicly available business information, such as disclosure of a FEIN, with no unauthorized disclosure of any PII?
◯	5. Other

Notes:

- Incidents that are **not** eligible for withdraw include:
  - Vendors or third-parties, where there is the possibility of a contractual or legal responsibility for the incident to the State; or
  - Any educational organization, whether it is a county board of education or institution of higher education, and is covered by cyber-insurance through BRIM.
- [1]An example would be having a non-SOWV entity disclosing unrequested PII to an unauthorized state workforce member.

- [2] Examples include requests for technical help that should have been submitted to the service desk, power or phone outages that have no security or privacy implications, or phishing attempts that should have been reported to otphishing@wv.gov.
- A description of the circumstances that support the reason for the withdraw of the incident ***must be*** provided in the text box below.

Describe the circumstances that support withdraw here:

2.12 Has the Departmental Privacy Officer determined that the incident is fully resolved, and either qualifies as an event, or to be withdrawn? If yes, check box, initial, read instructions.

☐ Yes **DPO Initials:** _____

STOP Do not complete the rest of the PIRA. See Section 6 for submission instructions. If the reported incident cannot be classified as an Event or should be withdrawn, proceed to Question 2.13.

INCIDENT ELEMENTS (Mark all that apply.)

2.13 Identify the type of incident:

☐	Unauthorized Access (unintentional)
☐	Unauthorized Disclosure
☐	Unauthorized Access and Use (includes intentional access or use)
☐	Loss / Theft
☐	Security Only (other than loss or theft)[1]
☐	NA, Other (describe in question 2.15)

Note: [1] Examples of Security Only incidents include DoS or website attacks, or the mishandling of computer equipment (e.g. chain of custody issues) that are not believed to have privacy implications.

2.14 Identify the incident medium – PII Medium:

☐	Electronic Data (explain in 2.16 if the data is structured or unstructured)
☐	Paper Documents (explain in 2.16 if the data is structured or unstructured)
☐	Verbal

2.15 Identify the root cause of the incident:

☐	Human error
☐	Personal use, lack of judgment

☐	Malicious act–cyber attack
☐	Malicious act–cyber fraud only[1]
☐	Malicious act–personal conflict
☐	Malicious act–personal financial gain
☐	Malicious act–theft
☐	System glitch
☐	NA, Unknown

Notes: [1] Examples of Security Only incidents include DoS or website attacks, or the mishandling of computer equipment (e.g. chain of custoday issues) that are not believed to have privacy implications.

2.16 Describe the nature of each element indicated in Questions 2.13 – 2.15[1]

[1]Notes:
Examples of type of incident include: Database access permissions were set too broadly; Employee looked up the PII of a neighbor; Employee's car was stolen and the laptop was in the car.
Examples of medium include: Purpose of the data; database (name) that was accessed or accessible; form name, number and general description; etc.
Examples of root cause: Employee sent an email with PII to an outside contractor unencrypted; faulty code or software updates.

2.17 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:

2.18 If Question 2.17, is "Yes", in the text box below enter the date(s) when policy/procedure training was last taken by, or provided to, the employee(s) involved in the incident?

2.19 Identify the categories of unauthorized recipients.

☐	Internal SOWV (Exec. Branch / wv.gov network)
☐	Internal SOWV (Other / non-wv.gov network)

Identify the non Exec. Branch / non-wv.gov recipient organization below:

☐	External – Vendor, Business Partner
☐	External – Citizen or Client
☐	External – Unknown (A recipient of PII is confirmed, but the identity is not.)
☐	Other (Identify organization below. Also use for cyber fraud.):
☐	Unknown. (Select when it cannot be confirmed if there was any unauthorized recipient.)

Describe the circumstances and activities that resulted in an "Unknown" determination below:

2.20 Select the categories of affected individuals, then provide a count of each category. The total number must reflect the total number individuals affected.

	Category	Number Affected
☐	Citizens, Clients or Customers (Non-HIPAA)	
☐	HIPAA Covered (Patients, Members)	
☐	Employees[1]	
☐	Contractors – Internal	
☐	Vendor Employees	
☐	Other (Describe below):	
	Total	0
☐	Minors < 18 years old (break out from total above)	
☐	Non-WV residents (break out from total above)[2]	

Provide the State code for all affected non-WV residents here (e.g. CA, FL, NY) below:

☐	Number affected cannot be determined. Provide an estimated number or range, if possible. Otherwise, write-in "unknown" if an estimated range cannot be provided.	

Notes:
[1] HIPAA Covered entities should use this line for privacy incidents involving the PII of employees. These incidents are not covered by HIPAA unless the incident involves PHI of employees who are patients or members of the as HIPAA covered entity or business associate.
[2]Please inform the State Privacy Office, as soon as possible, if non-wv residents are affected. There could be other state laws that are applicable to the incident that have more stringent requirements.

2.21 Identify the types of PII involved in this incident (Mark all that apply):

☐	Full Name (First and Last)[1]	☐	Partial Name (First initial and Last) [1]
☐	Partial Name-Other (Describe below)	☐	Spouse or Child Information
☐	Social Security Number (Full) [1]	☐	Social Security Number (Partial)
☐	Driver's License Number[1]	☐	Home Address
☐	Financial Account Number with Access Code[1]	☐	Home Phone Number
☐	Protected Health Information (HIPAA)[2]	☐	Mobile Phone Number
☐	Mental Health/Substance Abuse Information	☐	Date of Birth
☐	Disability Status	☐	Identifying Photograph[3]
☐	Health Information (Non-HIPAA) [3]	☐	Financial Information (General)[3]
☐	Federal Tax Information[3]	☐	Employment Information[3]
☐	Payment Card Information[3]	☐	ID Number (non SSN, DLN) [3]
☐	Education Information[3] (FERPA covered, other)	☐	Other (Describe below) [3]

Notes:
[1]Combinations of these PII types may trigger the WV State Breach Code.
[2]Provide detail below on the types of PHI involved.
[3]Provide detail below on these types of PII involved.
Do not report the actual PII or PHI (e.g. diagnoses, medications) or describe sensitive information that could be identifying.

(2) **HIPAA only:** List the "types" of PHI involved (e.g. diagnoses, medications, labwork, account numbers, etc.) below:

(3) List the types of PII for the categories identified in Note 3 (e.g. tax return, full face photo, diagnosis, medications, health status, student ID or other FERPA covered information.):

2.22 Provide a description of any other aspects of the incident not covered above that are important to convey and document:

2.23 Provide the names of the individuals who participated in managing the incident response (include external individuals who helped mitigate incident):

2.24 Document the external professional resources used to manage the incident:

		Date[1]
Was the State's contracted breach coach engaged?	-Select-	
Was an external cyber security firm engaged for forensics?	-Select-	
Call Center	-Select-	

[1]Date of initial engagement for that resource. Dates can be provided by SPO if unknown.

SECTION 3 – INCIDENT MITIGATION DOCUMENTATION AND RISK ASSESSMENT

3.1 What actions were taken to resolve and/or mitigate the incident? Be specific.

RISK ASSESSEMENT

HIPAA EXCEPTION REVIEW – This section is *only* for HIPAA covered incidents (including business associates). *It is inactive unless Protected Health Information (PHI) is selected in 2.21.* For non-HIPAA incidents skip to Question 3.6:

Note: Breach exceptions are rare and narrowly defined. Only one breach exception is possible. If no exception applies, proceed to Question 3.6. If a breach exception applies, document the circumstances of why the exception applies in Question 3.5, then skip the risk assessment and continue with Section 4.

3.2 Breach Exception 1 – Unintentional Access, Acquisition or Use:

1. Was PHI unintentionally acquired, accessed or used by a workforce member or business associate?	-Select-
2. Was the workforce member acting in good faith and under the scope of their authority?	-Select-
3. Was the PHI further disclosed?	-Select-
4. HIPAA Breach Exception 1 applies if the answers are all Yes, Yes, and No.	-Select-

3.3 Breach Exception 2 – Inadvertant Disclosure:

1. Was PHI inadvertently disclosed by a covered entity (or business associate) workforce member who was authorized to access PHI?	-Select-
2. Was the disclosure made to a workforce member of the same covered entity (or business associate) who is authorized to access PHI?	-Select-
3. Was the PHI further disclosed?	-Select-
4. HIPAA Breach Exception 2 applies if the answers are all Yes, Yes, and No.	-Select-

3.4 Breach Exception 3 – PHI Retention Status:

1. Is there a good faith belief that the unauthorized person to whom the disclosure of PHI was made would not reasonably be able to retain the information?	-Select-
2. HIPAA Breach Exception 3 applies if the answer is Yes.	-Select-

3.5 Document the circumstances of why the particular breach exception applies:

FOUR FACTOR RISK ASSESSMENT – This section is for ***all incidents***, except incidents determined to be an "event" in Question 2.8 or have a documented HIPAA EXCEPTION in Questions 3.2 - 3.4.

3.6 Factor 1: Nature and extent of PII/PHI accessed, acquired, disclosed or used:

1. Did this involve a significant number of PII/PHI identifiers?	-Select-
2. How many direct identifiers were involved?	
3. Were sensitive identifiers involved, such that they could be used to commit identity theft or other financial harm? (e.g. SSN, DLN, Financial Acct. #, Medical Acct. #)	-Select-
4. Were identifiers involved that could be used to locate the affected individual(s)? (e.g. Address, Home or Mobile Phone #, Employment Information)	-Select-
5. If only indirect identifiers were involved were they of a such a nature, or of sufficient number, that re-identification is likely?	-Select-
6. Did the PII/PHI involve a sensitive diagnoses? (e.g. HIV, STDs, Substance Abuse and/or Mental Health, or Medications that indicate a sensitive diagnosis)	-Select-
7. Does the PII/PHI relate to a well-known individual (either locally or nationally)?	-Select-
8. Does Factor 1 support a low risk of compromise, harm? *(To answer 3.6.8, only consider the nature and extent of the PII/PHI. Do not consider any of the other factors.)*	-Select-

3.7 Factor 2: Nature of Recipient(s):

Section 1 - For *all* incidents answer all applicable questions:

1. True or False: PII/PHI was accessible or potentially acquired, but it is unknown if it was accessed, viewed or exfiltrated. (e.g. incorrectly set access privileges)	-Select-
2. Was each recipient authorized to receive the PII/PHI? (e.g. intended recipient of unencrypted email)	-Select-
3. Were all recipients contacted to help with mitigation? If not, explain below.	-Select-
4. Does each recipient have a relationship to the affected individual, such that they are likely to act in the individual's best interest? (e.g. family, friend, caregiver)	-Select-
5. Are the unauthorized recipients trusted individuals with professional or legal obligations to protect the privacy and security of the disclosed PII/PHI? (e.g. staff of a HIPAA covered entity, or licensed professional, such as an attorney or CPA)	-Select-
6. Did the unauthorized recipients contact your agency to report the receipt of the PII/PHI?	-Select-
7. Has any unauthorized recipient conducted themselves in a manner that would indicate a lack of trustworthiness?	-Select-
8. Has any unauthorized recipient used the PII/PHI in any malicious act, or other manner that would benefit the recipient?	-Select-
9. Has each unauthorized recipient fully cooperated with mitigation requests by returning, securing or destroying documents with PII/PHI?	-Select-
10. Does any unauthorized recipient have the know-how or resources to re-identify affected individual(s) if only indirect identifiers were disclosed?	-Select-
11. Did any recipient unintentionally, further disclose the PII/PHI to unauthorized individuals? If yes, incorporate the additional disclosure and mitigation efforts in all applicable questions.	-Select-

Section 2 - *Only applicable when recipients are SOWV workforce members (incl. contractors, vendors):*

12. Is there a signed executive branch confidentiality agreement on file for each unauthorized recipient? Or...	-Select-
13. ...If any unauthorized recipients are a contract worker, employed by a vendor, or a business partner are they trusted individuals with a contractual or legal obligation to protect the privacy and security of the disclosed PII/PHI?	-Select-
14. Does Factor 2 support a low risk of compromise and harm? *(To answer 3.7.14, only consider the nature or characteristics of the recipients. Do not consider any of the other factors.)*	-Select-

3.8 Factor 3: Extent of the Acquisition or Viewing:

1. Was this an intentional act done for personal gain or malicious harm?	-Select-
2. Was PII/PHI confirmed to have been acquired? Or...	-Select-
3. ...Was PII/PHI potentially heard, viewed or acquired? If yes, please explain below.	-Select-
Explain the circumstances of the potential hearing, viewing or acquisition below:	
4. Was a digital forensic analysis completed that documents the extent of the acquisition or viewing?	-Select-
5. What investigational discoveries support the above conclusions (e.g. digital forensics; audit reports; oral or written testimony)? Describe below:	
6. Does Factor 3 support a low risk of compromise and harm? *(To answer 3.8.6, only consider the extent of the unauthorized acquisition or viewing of PII/PHI. Do not consider any of the other factors?)*	-Select-

3.9 Factor 4: Risk Mitigation

1. Was verbal confirmation received from each unauthorized recipient that the PII/ PHI was thoroughly deleted, destroyed, or returned, and will not be further used or disclosed?	-Select-
2. Was the verbal confirmation received thoroughly documented as to the manner, date, time and individual by whom it was provided?	-Select-
3. Was written confirmation received from each unauthorized recipient that the PII / PHI was thoroughly deleted, destroyed, or returned, and will not be further used or disclosed?	-Select-
If yes, provide the type of written confirmation below (e.g. email, memo, letter, signed affidavit, witnessed affidavit, or notarized affidavit):	
4. Was the PII/PHI thoroughly deleted, destroyed, or returned within an appropriate amount of time?	-Select-
5. Was data wiped remotely?	-Select-

6. If mitigation efforts were unsuccessful in getting the PII/PHI deleted, destroyed, or returned, are there other circumstances that might demonstrate successful mitigation?	-Select-
Explain successful and unsuccessful risk mitigation efforts, including factors that support the above answers:	
7. Does Factor 4 support a low risk of compromise and harm? *(To answer 3.9.7, only consider the successfulness of the risk mitigation efforts. Do not consider any of the other factors.)*	-Select-

3.10 Review of Four Factor Risk Assessment:

1. Do Factors 1 – 3 all point to a low risk of compromise and harm?	-Select-
2. Does Factor 4 mitigate any non-low risk of compromise or harm in Factors 1-3? *If yes, notification is not likely.*	-Select-
3. Overall Assessment: Based on the above four-factor risk analysis, is it reasonable to determine this incident can be categorized as a low-risk incident under the HIPAA Privacy and Security Rules, W. Va., Code § 46A-2A-101, or any other applicable privacy statutes and regulations, such as the PCI DSS?	-Select-

SECTION 4 – NOTIFICATION SUMMARY

Instructions related to 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, contact ashley.e.summitt@wv.gov, lori.l.tarr@wv.gov; or, lora.m.reynolds@wv.gov.

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

4.1 Non-HIPAA Notification Summary (W. Va. Code § 46A-2A-101)**:**

○	Due to a low risk of harm, notification is not required, or is otherwise not applicable.
○	Due to a high risk of harm, notification is required by WV Breach Law.
○	Notification is not mandated by law, but appropriate for the circumstances. Provide a detailed description of why notification should be made below:

Date(s) of notification to individuals. Provide a list all dates, and the number of letters sent on each date below:
If notification was not made by letter describe method (e.g. Email, Telephone), and explain why:

4.2 HIPAA Notification Summary (45 C.F.R. §§ 164.400-414)**:**

○	Due to a low risk of compromise, or a qualified exception, notification is not required.
○	Due to a medium or high risk of compromise, notification is required under HIPAA. 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.

Date(s) of notification to individuals. Provide a list all dates, and the number of letters sent on each date below:
If applicable, provide the date of notification to the Office of Civil Rights here:[1]

[1] If notification to OCR has not yet been made, read, check and initial the statement below affirming the knowledge that notification to OCR must be made according to all Breach Notification Rule requirements.

☐ I understand that this incident must be reported, without unreasonable delay, to the Office of Civil Rights pursuant to 45 C.F.R. § 164.408, with the aid of the State Privacy Office. And,

- For incidents with fewer than 500 affected individuals, the incident must be reported no later than within 60 days after the end of the calenday year in which the breach was discovered.
- For incidents with 500 or more affected individuals the incident must be reported no later than 60 days from the discovery of the breach.

DPO Initials here:

4.3 Special Notifications (other than HIPAA or W. Va. Code § 46A-2A-101)**:**

☐	Special Notification (SSA, PCI, FTI, etc.): Due to compliance with other laws or industry standards notification was made.

Specify laws or industry standards here:
Describe notification requirements below:
Date(s) of Notification:

4.4 Was credit monitoring provided? -Select-

# of Adults:

# of Minors:

SECTION 5 – INCIDENT OUTCOME

5.1 What measures have been, or will be, implemented to prevent this type of incident from reoccurring? (Mark 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):

5.2 Beyond notification, what was the outcome of the incident? Please be specific, and describe measures indicated in 5.1.

SECTION 6 – Filing Instructions for PIRA Submissions

1. PIRA must be kept in fillable pdf format.
2. Submit by email according to the following:
    a. Subject line format**: PIRA for Incident <insert SPO#>, < insert OT Tracking Number#>**
    b. Send to:
        i. State Privacy Office
            1. ashley.e.summitt@wv.gov
            2. lori.l.tarr@wv.gov
            3. lora.m.reynolds@wv.gov
        ii. WVOT Cyber Security Office – cso@wv.gov
        iii. Cabinet Secretary
        iv. Others as applicable
3. If you are submitting a draft for pre-submission review, please add **"Draft"** to the beginning of the subject line.

SECTION 7 – This space is for additional information if needed, and may also be used by the State Privacy Office. If any significant note is added, or change is made, the DPO will be notified.