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): _____

How was incident reported?

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

_____

Was incident reported to law enforcement? If yes, attach copy of report. If the report is not available, identify the law enforment agencies to which a report was made. (Mark all that apply.)

☐	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, and for non-WVSP, 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):

Event Classification or Incident Withdraw Determination

Event: Questions 2.8 – 2.10, and 2.12 are used to determine and document that an incident may be classified as an ***event.***

Withdrawn: Questions 2.11 and 2.12 are used to determine and document why a reported incident may be ***withdrawn***. To withdraw an incident, it must be previously approved by the State Privacy Office in writing.

*Skip to Question 2.13 – **Incident Elements**, if you know that this incident cannot be classified as an event, or it was not withdrawn.*

2.8 Encryption status:

Does this incident involve an email that was sent *unencrypted*? If yes, proceed to Question 2.13	
Non-HIPAA: Was the data containing Personally Identifiable Information (PII) encrypted[1], rendering the data elements unusable, unreadable or indecipherable?	
HIPAA: Was the data containing PHI encrypted per NIST standards or other encryption process similarly effective to the NIST standard?[1,2]	

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 the PII status for encryption is "Yes", then 2.13 is also "Yes."

2.9 Classification determination when encryption is not a factor:

Was PII accessible by an unauthorized individual?	
Was PII disclosed to an unauthorized individual?	
Was PII used, modified, or destroyed in an unauthorized manner?	

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 that do not involve encryption, describe the following:

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

2.11 Withdraw of incident determination:

Was this a reported incident that was determined to be caused by: 1. the individual whose PII was involved, or 2. an external organization outside the State of West Virginia that has the responsibility of managing the incident?[1]	
Was this a reported incident that was determined to not be privacy or security related, or otherwise errantly reported?[2]	
Was this a reported incident that included only publicly available business information, such as a disclosure of a FEIN, with no unauthorized disclosure of any PII?	

Notes:

- This exclusion does **not** apply to incidents involving:
  - Vendors or third-parties, where there could be a contractual or legal responsibility for the incident; or
  - Any educational organization, whether it is a higher education organization or county board of 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 outages or phone problems that have no security or privacy impacts, and phishing attempts that should have been reported to otphishing@wv.com.
- A description of the circumstances that support the decision to withdraw the incident ***must be*** provided in the text box below.
- If any question in 2.11 can be answered "Yes", then 2.12 is also "Yes."

Describe the circumstances that support withdraw here:

2.12 Has the Departmental Privacy Officer determined that the incident is fully resolved and is only an event or should be withdrawn?

☐ Yes | **DPO Initials:** _____

If 2.12 is "Yes" stop here. 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 custoday issues) that are not believed to have privacy implications.

2.14 Identify the incident medium – PII Medium:

☐	Electronic Data
☐	Paper Documents
☐	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.) ☐

If Yes, indicate by name and number:

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

Date:

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. Confirmation of a recipient could not be made for this incident.

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

2.20 Identify and mark the categories of affected individuals, and provide a count of each category.

	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]	☐	Spouse or Child Information
☐	Partial Name (First initial and Last) [1]	☐	Home Address
☐	Social Security Number (Full) [1]	☐	Home Phone Number
☐	Driver's License Number[1]	☐	Mobile Phone Number
☐	Financial Account Number with Access Code[1]	☐	Date of Birth
☐	Protected Health Information (HIPAA)[2]	☐	Social Security Number (Partial)
☐	Mental Health/Substance Abuse Information	☐	Partial Name-Other (Describe below)
☐	Disability Status	☐	Identifying Photograph[3]
☐	Health Information (Non-HIPAA) [3]	☐	Financial Information[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 Diagnosis, Medications
Do not report the actual PII, PHI or describe any sensitive identifying information.

(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, Student ID or other F):

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?		
Was an external cyber security firm engaged for forensics?		
Call Center		

[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). 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 – Unintential Access, Acquisition or Use:

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

3.3 Breach Exception 2 – Inadvertant Disclosure:

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

3.4 Breach Exception 3 – PHI Retention Status:

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?	
HIPAA Breach Exception 3 applies if the answer is Yes.	

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:

Did this involve a significant number of PII/PHI identifiers?	
How many direct identifiers were involved?	
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. #)	
Were identifiers involved that could be used to locate the affected individual(s)? (e.g. Address, Home or Mobile Phone #, Employment Information)	
If only indirect identifiers were involved were they of a such a nature or of suffficient number that re-identification is likely?	
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)	
Does the PII/PHI relate to a well-known individual (either locally or nationally)?	
Does Factor 1 support a low risk of compromise, harm? *(Only consider questions related to the nature and extent of the PII/PHI. Do not consider any of the other factors.)*	

3.7 Factor 2: Nature of Recipient(s):

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

True or False: There are no known recipients, but there is a possibility that PII/PHI was accessed or acquired. (e.g. database permissions allows unauthorized access.)	
Were the recipients authorized to have or view the PII/PHI? (e.g. intended recipients of unencrypted email)	
Were all recipients contacted to help with mitigation? If not, explain why not below.	
Explain why unauthorized recipients were not contacted below:	
Does an unauthorized 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 of client or patient)	
Are the recipients trusted individuals with professional or legal obligations to protect the privacy and security of the disclosed PII/PHI? (e.g. licensed professional or staff of a HIPAA covered entity, attorney or member of the court, CPA)	
Has any recipient conducted themselves in a way that would indicate a lack of trustworthiness?	
Has any recipient used the PII/PHI in any malicious act, or other manner that would benefit the recipient?	
Have the recipients fully cooperated with mitigation requests by returning, securing or destroying documents with PII/PHI?	
Are any of the recipients individuals that have the know-how or resources to re-identify the affected individual(s) if only indirect identifiers were disclosed?	
Did any recipient unintentionally, further disclose the PII/PHI to unauthorized individuals? If yes, detail the additional disclosure in Question 2.21 and include it in the risk assessment factors.	

Section 2 - For incidents with SOWV workforce recipients (incl. contractors, vendors):

Is there a signed executive branch confidentiality agreement on file for each recipient?	
Are the recipients trusted employees of a vendor, contract workers or other business partners with contractual or legal obligations to protect the privacy and security of the disclosed PII/PHI?	
Does Factor 2 support a low risk of compromise and harm? *(Only consider questions related to the nature or characteristics of the recipients. Do not consider any of the other factors.)*	

3.8 Factor 3: Extent of the Acquisition or Viewing:

Was this an intential act done for personal gain or malicious harm?	
Was PII/PHI acquired?	
Was PII/PHI potentially heard, viewed or acquired? If yes, please explain below.	
Explain the circumstances of the potential hearing, viewing or acquisition below:	
Was a digital forensic analysis completed that documents the extent of the acquisition or viewing?	
What investigational discoveries support the above conclusions (e.g. digital forensics; audit reports; oral or written testimony)? Describe below:	
Does Factor 3 support a low risk of compromise and harm? *(Only consider questions related to the extent of the unauthorized acquisition or viewing of PII/PHI. Do not consider any of the other factors?)*	

3.9 Factor 4: Risk Mitigation

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

If mitigation efforts were unsuccessful in getting the PII/PHI deleted, destroyed, or returned, are there other circumstances that might demonstrate successful mitigation?	
Explain successful and unsuccessful risk mitigation efforts, including factors that support the above answers:	
Does Factor 4 support a low risk of compromise and harm? *(Only consider questions related to risk mitigation of the PII/PHI. Do not consider any of the other factors.)*	

3.10 Review of Four Factor Risk Assessment:

Do Factors 1 – 3 all point to a low risk of compromise and harm? *If yes, notification is not likely.*	
Does Factor 4 mitigate any non-low risk of compromise or harm in Factors 1-3? *If yes, notification is not likely.*	
Overall Assessment: Based on the above 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.	

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, tara.l.taylor@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)**:** Reset Section

○	1. Due to a low risk of harm, notification is not required; or 2. Notification is 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 made by a format other than a letter describe below, and why (e.g. Email, Telephone):	

4.2 HIPAA Notification Summary: Reset Section

○	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. 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:	

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 What was the outcome of the incident? Please be specific, and describe measures indicated in 5.1.

SECTION 6 – Filing Instructions

1. Submit the PIRA by email with the following Subject line**:**
   PIRA Submission for Incident <SPO#>, < OT Tracking Number#>

   Note: If submitting a draft to our office for review, please add "Draft" to the beginning of the subject line.

2. Send to:
   a. State Privacy Office
      i. ashley.e.summitt@wv.gov
      ii. lori.l.tarr@wv.gov
      iii. tara.l.taylor@wv.gov
   b. Cyber Security Office – cso@wv.gov
   c. Cabinet Secretary
   d. Others as applicable

SECTION 7 – This space is for additional information if needed

CLEAR FORM