

West Virginia Executive Branch

Procedure: **Response to Unauthorized Disclosures**

Issued by: **Sonia Chambers**
West Virginia Health Care Authority

Procedure No: WVEB-P101.1 Issue Date:06/01/09 Effective Date: 09/01/09 Rev. Date:

Page 1 of 8

1.0 PROCEDURE

This procedure provides the basis of appropriate response to events that may expose personally identifiable information (PII) to unauthorized internal or external persons.

This procedure defines an Unauthorized Disclosure, describes the responsibilities of Executive Branch Department personnel in connection with Unauthorized Disclosures, and outlines the steps they must take to ensure that Unauthorized Disclosures are properly reported, contained, investigated, and mitigated.

2.0 SCOPE

This procedure applies to all Departments (including Agencies, Boards, and Commissions) within the Executive Branch of the West Virginia State Government, excluding constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, County Boards of Education, and Public Service Commission. However, the Privacy Office recommends that all Agencies, including those excluded above, follow this procedure.

3.0 REQUIREMENTS

3.1 Defining Unauthorized Disclosure

3.1.1 An Unauthorized Disclosure is any disclosure of PII that is not an Authorized Disclosure.

3.1.2 An Authorized Disclosure is a disclosure of PII to:

- a) Individuals within the Department who have a need to know the PII to conduct Department business;
- b) Third parties who process the PII on the Department's behalf, provided that these third parties have a contractual or legal duty to protect the PII;

West Virginia Executive Branch

Procedure: **Response to Unauthorized Disclosures**

Issued by: **Sonia Chambers**

West Virginia Health Care Authority

Procedure No: WVEB-P101.1 Issue Date:06/01/09 Effective Date: 09/01/09 Rev. Date:

Page 2 of 8

- c) Third parties who provide legal, accounting and other advisory services to the Department, provided that these third parties have a contractual or legal duty to protect the PII;
- d) Other government agencies, for legally required or authorized purposes;
- e) The individual to whom the PII pertains, or the individual who provided the PII to the Department (such as to an employee who has provided family-member PII for benefits purposes) in accordance with the Individual Rights Policy, and
- f) Any person, if the Department is required by law to make the disclosure (such as in response to FOIA requests) or if the individual to whom the PII pertains consents to the disclosure.

3.1.3 There are two possible types of Unauthorized Disclosures:

3.1.4 An Internal Unauthorized Disclosure: occurs when PII is exposed or potentially exposed to any person(s) within the Executive Branch; and

3.1.5 An External Unauthorized Disclosure: occurs when PII is exposed or potentially exposed to any person(s) outside of the Executive Branch.

3.1.6 Any known or suspected Unauthorized Disclosures (accidental or otherwise) must be immediately reported in accordance with Section 4.0 of this procedure for appropriate investigation and handling. This reporting requirement applies both to Internal Unauthorized Disclosures and to External Unauthorized Disclosures.

3.2 Examples of Unauthorized Disclosures: (List is not exhaustive)

3.2.1 Loss or theft of paper records containing PII, such as loss or theft of a briefcase containing papers with PII;

West Virginia Executive Branch

Procedure: **Response to Unauthorized Disclosures**

Issued by: **Sonia Chambers**

West Virginia Health Care Authority

Procedure No: WVEB-P101.1 Issue Date:06/01/09 Effective Date: 09/01/09 Rev. Date:

Page 3 of 8

- 3.2.2 Loss or theft of physical IT assets including computers, storage devices (such as flash drives), or storage media (such as CDs) that contain PII;
- 3.2.3 Loss or theft of a personal PDA, mobile devices or flash drives containing PII;
- 3.2.4 Improper disposal of records, media or equipment containing PII;
- 3.2.5 Accidental or intentional transmission of PII to the wrong person, such as a file being emailed to the wrong recipient;
- 3.2.6 Loss of PII during transit, such as packages that are lost or misdelivered;
- 3.2.7 Loss of control of PII, such as an inability to locate computers or storage media;
- 3.2.8 Discovery of viruses, spyware or malicious code that intercepts PII;
- 3.2.9 Discovery of unauthorized access to systems containing PII; or
- 3.2.10 Transmission of PII to an unauthorized vendor or agency.

4.0 PROCEDURE

- 4.1 All workers and contractors who access state systems, networks and facilities are to immediately report Level One Unauthorized External Disclosures (See 4.4.4) to the Office of Technology (OT) Service Desk @ 1-304-558-9966 or 1-877-558-9966 and their supervisor and/or Manager. This is the default process unless the Secretary or Agency Head creates an alternative reporting system through procedure, which shall include notification of the State Privacy Office. Provide the following information about the incident (or as much as is known):
 - 4.1.1 The date the incident occurred (if known) or was discovered;
 - 4.1.2 What PII was exposed;

West Virginia Executive Branch

Procedure: **Response to Unauthorized Disclosures**

Issued by: **Sonia Chambers**

West Virginia Health Care Authority

Procedure No: WVEB-P101.1 Issue Date:06/01/09 Effective Date: 09/01/09 Rev. Date:

Page 4 of 8

4.1.3 What steps (if any) have been taken to recover the PII; and

4.1.4 Any other information that may be relevant.

4.2 The Department Privacy Officer or designee shall notify the State Privacy Office of the incident.

4.3 For any Unauthorized Disclosure that involves OT systems, the person receiving the report shall notify OT in accordance with OT incident response procedures.

4.4 Once notified of an Unauthorized Disclosure, the Privacy Officer (or designee) shall:

4.4.1 Ensure that OT or other appropriate personnel have been notified so that they can take the steps needed to close any security gaps. For example, affected systems have been isolated, processes that expose PII have been terminated, etc.

4.4.2 Oversee efforts to recover exposed PII. If PII is recovered, document the basis for any belief that the PII will not be misused.

4.4.3 Activate the Department response team.

4.4.4 Classify the Unauthorized Disclosure as follows:

- a) Level 3 Disclosure – Unauthorized Internal Disclosure of PII does not contain any Sensitive PII.
- b) Level 2 Disclosure – Unauthorized Internal Disclosure of Sensitive PII or Unauthorized External Disclosure of PII that does not contain any Sensitive PII.
- c) Level 1 Disclosure – Unauthorized External Disclosure, for purposes of this categorization, “Sensitive PII” means any PII containing Social Security numbers, driver’s license numbers, payment card numbers,

West Virginia Executive Branch

Procedure: **Response to Unauthorized Disclosures**

Issued by: **Sonia Chambers**

West Virginia Health Care Authority

Procedure No: WVEB-P101.1 Issue Date:06/01/09 Effective Date: 09/01/09 Rev. Date:

Page 5 of 8

financial account numbers, insurance account numbers, medical information or PHI, and biometric data.

- 4.4.5 Notify Department leaders, per established procedures. (Notification should include individuals responsible for insurance coverage).
- 4.4.6 If the incident may be the result of criminal activity, notify law enforcement or confirm that law enforcement has been notified by OT.
- 4.4.7 If Payment Card Industry data is exposed, notify appropriate financial institutions in accordance with PCI Data Security Standards. The standards apply to all organizations that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions. A company processing, storing, or transmitting cardholder data must be PCI DSS compliant.
- 4.4.8 If PHI is exposed, notify individuals, the media and HHS in accordance with HIPAA obligations.
- 4.4.9 Prepare inventory of exposed data elements.
- 4.4.10 Analyze possible risks to the affected individuals as a result of the Unauthorized Disclosure. Determine how any risks can be minimized.
- 4.4.11 If nature of the incident cannot be fully determined using Department and/or OT resources, contract with forensics professionals as needed.
- 4.4.12 Determine whether to notify impacted individuals in accordance with WV SB 340, W.Va. Code §46A-2A-101, et seq., concerning electronic data transfer, assess:

Do the data elements include: (a) a West Virginia resident's first name or first initial and last name and (b) linked to SSN, driver's license number or state ID card, or financial account number, credit card or debit card number, along with

West Virginia Executive Branch
Procedure: **Response to Unauthorized Disclosures**
Issued by: **Sonia Chambers**
West Virginia Health Care Authority

Procedure No: WVEB-P101.1 Issue Date:06/01/09 Effective Date: 09/01/09 Rev. Date:

Page 6 of 8

the required security code, access code or password? If yes, then determine whether: (c) the data is unencrypted or unredacted and (d) whether the data was or is reasonably believed to have been accessed acquired by an unauthorized person and that causes, or it is reasonably believed that it has caused or will cause, identity theft or other fraud. If the answer is yes, then notify impacted individuals. If no, then consider (a) and (b) below.

- a) If encrypted data elements are exposed, and are accessed and acquired in an unencrypted form or if they are exposed to an individual with access to the encryption key, and it is believed that the breach has caused or will cause identity theft or other fraud, then notify impacted individuals. For example a laptop is encrypted, but is lost after the user signs on; the information is now available in unencrypted format and is accessed before the user signs out.
- b) The Secretary or Agency Head has inherent authority to use discretion to notify in situations not identified above.

- 4.4.13 Note: Individual notification may be delayed if a law enforcement agency advises that notification would impede an investigation or security.
- 4.4.14 Prepare a list of affected individuals. If incident is (or may be) a Level 1 Disclosure, determine if current contact information for individuals is available to support formal written notification. Use of last known postal address in the Department's records shall be utilized, if notification is accomplished through mailing. Notification may also be accomplished via email or telephone; substitute notice may also be appropriate, see W. Va. Code §46A-2A-101 (7)(D).
- 4.4.15 Identify applicable legal statutes and determine risks associated with violations of the laws.
- 4.4.16 Develop notification plan for Department workers; issue statement reminding workers to refer all questions to the Privacy Officer.
- 4.4.17 Develop standby statement for media.

West Virginia Executive Branch
Procedure: **Response to Unauthorized Disclosures**
Issued by: **Sonia Chambers**
West Virginia Health Care Authority

Procedure No: WVEB-P101.1 Issue Date:06/01/09 Effective Date: 09/01/09 Rev. Date:

Page 7 of 8

- 4.4.18 Create communications outline containing:
- a) Basic facts (what happened, what data was exposed, to whom);
 - b) Steps the Department is taking to mitigate harm;
 - c) Steps the Department is taking to prevent reoccurrence; and
 - d) Provide an expression of regret and empathy for the situation.
- 4.4.19 Determine Department leader who will deliver messages and obtain media training if necessary.
- 4.4.20 Create FAQ to support communications program.
- 4.4.21 For Level 1 Incident, draft individual notification letters (per security breach notification law):
- a) If more than 1,000 individuals must be notified, then the three consumer reporting agencies must also be notified. They can be notified at the following websites:
 - Equifax (800) 525-6285
<http://www.equifax.com>
 - Trans Union (800) 971-4307
<http://www.transunion.com>
 - Experian (888) 397-3742
<http://www.experian.com>
 - b) Determine how questions from affected individuals will be managed. For example, designate an email address, post FAQs on webpage, take calls at an existing phone number, establish call center.

West Virginia Executive Branch

Procedure: **Response to Unauthorized Disclosures**

Issued by: **Sonia Chambers**

West Virginia Health Care Authority

Procedure No: WVEB-P101.1 Issue Date:06/01/09 Effective Date: 09/01/09 Rev. Date:

Page 8 of 8

- c) If center is authorized, obtain toll-free number, train personnel on messages.
- d) Print and mail letters when authorized. In the few situations when the contracted vendor is visible to the impacted individual(s), Departments may request the vendor to take responsibility for notification.
- e) Track response and update FAQs, call center training as needed.

4.4.22 For Level 2 and Level 3 breaches, determine what (if any) individual communications are needed. For example, if workers are generally aware that “something has happened” it may be prudent to provide a notice to minimize the risks of misinformation/speculation. In these cases, notice may be provided in any manner that makes sense given the situation.

4.4.23 Conduct a post-incident review to determine what steps can be taken to prevent reoccurrence. Document and distribute analysis of the underlying incident and the response to facilitate organizational learning.

4.4.24 The Department Privacy Officer is responsible for providing a completed Privacy Incident Report to the State Privacy Office, Chief Technology Officer and Department Cabinet Secretary within 30 days of the incident, as applicable.

4.4.25 The Privacy Officer may also recommend additional specific controls or improvements to the Privacy Program, including additional training.

5.0 ENFORCEMENT

Any employee found to have violated this procedure may be subject to disciplinary action up to and including dismissal. Disciplinary action, if determined to be necessary, will be administered by the employing Department and may be based on recommendations of the Privacy Office.

6.0 DEFINITIONS

Refer to Privacy Office Glossary