

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: 5/21/10
Page 1 of 9

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. It also has been updated to include procedures for breaches of PHI, pursuant to HIPAA.¹

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 the 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:

¹ References to HIPAA shall mean 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"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA").

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

Procedure No: WVEB-P101.1
Page 2 of 9

Issue Date: 06/01/09

Effective Date: 09/01/09

Rev. Date: 5/21/10

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

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

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

Procedure No: WVEB-P101.1
Page 3 of 9

Issue Date: 06/01/09

Effective Date: 09/01/09

Rev. Date: 5/21/10

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 Unauthorized Internal Disclosures, and to Unauthorized External 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;
- 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.

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

Procedure No: WVEB-P101.1
Page 4 of 9

Issue Date: 06/01/09

Effective Date: 09/01/09

Rev. Date: 5/21/10

4.0 PROCEDURE

- 4.1 All workers, supported by the Office of Technology (OT) and contractors who access state systems, networks and facilities are to immediately report Level 1 Unauthorized Disclosures (See 4.5.4) to the OT Service Desk @ 1-304-558-9966 or 1-877-558-9966, or <http://www.technology.wv.gov/security/Pages/reportacomputersecurityincident.aspx> and their supervisor and/or Manager. Level 1 Unauthorized Disclosures may include incidents involving electronic, paper or verbal information. 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;
 - 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 OT will evaluate whether any PII or PHI is impacted by the incident and will notify the State Privacy Office of the same. The State Privacy Office will then notify the appropriate Department Privacy Officer. If, for whatever reason, the Department Privacy Officer first learns of the incident, he or she or designee shall notify the State Privacy Office of the incident, which shall then notify OT.
- 4.3 Department Privacy Officers are encouraged to develop their own procedures for reporting of all other Unauthorized Disclosures.
- 4.4 For any Unauthorized Disclosure that involves OT systems, the person receiving the report shall notify OT in accordance with OT incident response procedures.

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: 5/21/10
Page 5 of 9

- 4.5 Once notified of an Unauthorized Disclosure, the Privacy Officer (or designee) shall:
 - 4.5.1 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.
 - 4.5.2 Oversee efforts to recover exposed PII. If PII is recovered, document the basis for any belief that the PII will not be misused.
 - 4.5.3 Activate the Department response team.
 - 4.5.4 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 (excluding PHI) 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, financial account numbers, insurance account numbers, medical information or PHI, and biometric data. Level 1 Disclosure also includes Unauthorized Internal Disclosure of PHI.
 - 4.5.5 Notify Department leaders, per established procedures. (Notification should include individuals responsible for insurance coverage).
 - 4.5.6 If the incident may be the result of criminal activity, notify law enforcement or confirm that law enforcement has been notified by OT.

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

Procedure No: WVEB-P101.1
Page 6 of 9

Issue Date: 06/01/09

Effective Date: 09/01/09

Rev. Date: 5/21/10

- 4.5.7 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.
- 4.5.8 If PHI is exposed, go to Appendix A regarding your HIPAA obligations. If data elements include those listed in § 4.5.12 of this Procedure, then compliance with both HIPAA and W. Va. Code § 46A-2A-101 is required; therefore, follow the remainder of this Procedure, as applicable.
- 4.5.9 Prepare inventory of exposed data elements.
- 4.5.10 Analyze possible risks to the affected individuals as a result of the Unauthorized Disclosure. Determine how any risks can be minimized.
- 4.5.11 If nature of the incident cannot be fully determined using Department and/or OT resources, contract with forensics professionals as needed.
- 4.5.12 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 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 and 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.

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: 5/21/10
Page 7 of 9

- 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.
- 4.5.13 Note: Individual notification may be delayed if a law enforcement agency advises that notification would impede an investigation or security.
- 4.5.14 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).
- 4.5.15 Identify applicable legal statutes and determine risks associated with violations of the laws.
- 4.5.16 Develop notification plan for Department workers; issue statement reminding workers to refer all questions to the Privacy Officer.
- 4.5.17 Develop standby statement for media.
- 4.5.18 Create communications outline containing:
- a) Basic facts (what happened, what data was exposed, to whom);

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: 5/21/10
Page 8 of 9

- 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.
- 4.5.19 Determine Department leader who will deliver messages and obtain media training if necessary.
- 4.5.20 Create FAQ to support communications program.
- 4.5.21 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.
 - c) If center is authorized, obtain toll-free number, train personnel on messages.

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: 5/21/10
Page 9 of 9

- 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.
- 4.5.22 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.
- 4.5.23 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.
- 4.5.24 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. Any breach notification log generated by the Department Privacy Officer pursuant to Appendix A, shall be submitted with the Report to the State Privacy Office immediately.
- 4.5.25 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)

Appendix A

DUTY TO REPORT SECURITY OR PRIVACY BREACH, NOTIFY AND MITIGATE THE EFFECT

RESPONSIBILITY:

Counsel, Administrators, Privacy and Security Officials

BACKGROUND:

A breach of Department's privacy or security policies or inappropriate use or disclosure of unsecured protected health information (PHI) may result in harm to the person who is the victim of the breach. It may also erode trust in an organization, and impair its ability to provide medical care. It is important to respond quickly to any alleged breach, to determine what occurred, to prevent a recurrence of any violation of policy or *law*, and to take steps to mitigate any harm. Under the HITECH ACT of ARRA it is also a requirement to act quickly and to report breaches of unsecured PHI to the individual (to whom the PHI belongs) as well as to the Secretary of Health and Human Services. NOTE: A breach is considered "discovered" as of the first day it is known to the covered entity or business associate (or when by exercising reasonable diligence, the issue would have been known to the organization). Further language in the Interim Final Rule indicates that "known to the covered entity" means when any person (other than the person committing the breach) who is a workforce member or agent of the covered entity is made aware of such breach is when the timeframe for notification begins. *Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for Department, is under the direct control of Department, whether or not Department pays them.

POLICY:

Department will determine if unsecured PHI was breached and follow federal and state laws to report such both to the affected individual and to the Secretary of the Department of Health and Human Services.

PROCEDURE:

1. The Department Response Team will conduct an immediate review to investigate and determine if the information breached was unsecured protected health information, and whether or not breach notification and mitigation must occur. The steps listed below should be taken in order to accomplish this objective.

2. Determine whether there has been a breach of unsecured PHI. This determination will be made in accordance with the DHHS Guidance document published in the Federal Register on April 27, 2009 which listed and described encryption and destruction as the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. This guidance is currently found at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>.
 - a. If the PHI is considered unsecured, go to Section 3 below.
 - b. If the PHI breached was considered secure (in accordance with the above Guidance document and the organization's use of technology), document such in your organization's compliance file and be sure to list what occurred and what steps were taken to address the issue and prevent its reoccurrence. Go to Section 9.
3. If after review, the PHI breached was considered unsecured, take the following steps:
 - a. Assess whether or not the security or privacy of the PHI was "compromised". "Compromised" means that the breach of PHI/data poses a significant risk of financial, reputational or other harm to the individual. If the PHI breached is considered "compromised" go to Section 4, below.
 - b. If the PHI breached is not considered "compromised", document such in your organization's compliance file, be sure to list what occurred and what steps were taken to address the issue and prevent its reoccurrence. Go to Section 9.
4. If the PHI breached is considered "compromised", determine if such use or disclosure of PHI meets the breach exclusions:
 - a. Unintentional access to PHI in good faith in the course of performing one's job and such access does not result in further impermissible use or disclosure.
 - b. Inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate or affiliated organized health care arrangement.
 - c. When PHI is improperly disclosed but the covered entity or business associate believes in good faith that the recipient of

the unauthorized information would not be able to retain the information.

5. If the PHI considered compromised meets one of the exclusions listed above, document such in your organization's compliance file and be sure to list what occurred and what steps were taken to address the issue and prevent its reoccurrence. This may include notifying legal counsel as appropriate. If an exclusion is met, go to Section 9.
6. Based on the analysis and resulting findings performed above, the Department Response Team will develop a plan to mitigate the harm, to the extent that this is practicable. Also follow Section 4.5.9 through Section 4.5.20 in the foregoing Procedure.
7. The Department Response Team will notify each affected individual(s) whose information has been inappropriately accessed, acquired or disclosed during such breach. If such breach was caused and identified by a business associate, it may be, based on the language within the business associate agreement, the business associate's responsibility to perform the following notification steps and to inform the covered entity of such (in accordance with the ARRA updated business associate contract).
 - a. Using the breach notification log, list the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed during such breach. This log will be submitted to the State Privacy Office, in accordance with Section 4.5.24 of the foregoing Procedure.
 - b. Once information has been validated, prepare to notify each individual within 60 days from discovering the breach. NOTE: All notification materials should be organized and maintained as the ability for Department to demonstrate its attempts at notification is an ARRA requirement.
8. Notification Steps to be followed:
 - a. Individual Notice Affecting 499 or Less Individuals
 - i. Individual notice must be provided via first class mail at the last known address.
 - ii. If the individual is deceased, the notice must be sent to the last known address of the next of kin, or personal representative. Department is only required to provide notice to the next of kin or personal representative; if it is known that the individual is deceased and has the address of the next of kin or personal representative.

iii. If there are 10 or less individuals for whom Department has insufficient or out-of-date contact information to provide the written notice Department is permitted to provide notice to such individuals through an alternative form of written notice, by telephone or other means e.g., email, even if the patient has not agreed to electronic notice.

iv. If there are 10 or more individuals where insufficient or *out of date contact information* exists, Department must provide a substitute notice by posting the notice for a period of 90 days, on the home page of its web site or by providing the notice in major print or broadcast media where the affected individual(s) likely reside. The notification must *include a toll-free number* for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

v. For fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

b. Breaches Affecting 500 or More Individuals

i. Individuals must be notified (same requirements for individual notice)

ii. Media Notice

1. Media must be notified (use same content and timeframe requirements as substitute individual notice, *including the toll-free number*) without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach.

2. Must be followed IF more than 500 residents of a State or jurisdiction are involved or if it is reasonable to believe information has been accessed, disclosed or acquired.

3. Notification to the media must be provided within the same timeframe as notice to the individual.

c. Notice to Secretary

i. In consultation with the appropriate Department Privacy Officer and the Director of Information Security, the State Privacy Office shall notify the Secretary of Health and Human Services electronically:

1. Concurrently with the notification sent to the individual and within 60 days if breach affects 500 or more individuals without regard to whether the breach involved more than 500 residents of a particular State or jurisdiction.

2. Annually (within 60 days after the close of the previous calendar year) if breach affects less than 500 individuals. The State Privacy Office may elect to notify the Secretary after each breach, thus avoiding additional record keeping and end of year reporting.
- ii. Business Associates of Executive Branch Departments shall only notify according to their Business Associate Agreement.

9. Steps for Breach of PHI:

- a. The allegation, the mitigation plan, mitigation actions taken, results, record of disciplinary actions (if any), breach notification materials (including letters and records of attempts to contact) and other supporting information will be documented by the Department Privacy Officer and Counsel, and the documentation will be retained for at least six years.
- b. If at any point breach notification is deemed unnecessary, the Cabinet Secretary or Agency Head has the inherent authority to decide whether or not to voluntarily notify the victim of the breach in order to mitigate effectively the alleged harm and in situations not identified above.
- c. Once all steps in the Appendix have been completed, go back to Procedure Section 4.5.21.

REFERENCE: **45 CFR § 164.530(f)**

See also: **SANCTIONS FOR VIOLATING PRIVACY AND SECURITY POLICIES AND PROCEDURES**