POLICIES AND PROCEDURES
TOPIC: Breach Notification
DOCUMENT NUMBER: 1500
EFFECTIVE DATE: January 30, 2014 **REVISED DATE:** February 22, 2015

WVHIN
WEST VIRGINIA HEALTH INFORMATION NETWORK

I. BACKGROUND AND PURPOSE

The purpose of this policy is to establish a notification process in compliance with the Health Information Technology for Economic and Clinical Health ("HITECH") Act and the HIPAA Privacy Rule for a Breach of Unsecured Protected Health Information. This notification process shall also comply with West Virginia law governing notice for breach of computerized personal information. Federal law is more stringent than applicable state law for Breaches of Unsecured Protected Health Information. Generally, Participating Organizations compliant with the requirements for Breach notification under federal law will also be compliant with state law requirements. For purposes of this Policy reference to the term Breach throughout will refer to Breaches as defined under the HITECH Act, the HIPAA Privacy Rule, and West Virginia law.

II. POLICY

Both federal and state laws protect Patients from the improper acquisition, access, use, or disclosure of their Protected Health Information by unauthorized persons and entities. In its performance of the functions of a Health Information Exchange, the WVHIN may receive and exchange a Patient's Protected Health Information from one Participating Organization to another. Although the WVHIN's Health Information Exchange may not be directly involved in Treatment or any other Permissible Use of this Protected Health Information, its electronic receipt and transport of this data qualifies it under the law as a Business Associate to its Participating Organizations. This status of a Business Associate places obligations upon the WVHIN if a Patient's Protected Health Information should ever be the subject of a Breach when residing in or passing through its Health Information Exchange.

A Breach occurs if Protected Health Information is acquired, accessed, used, or disclosed by an unauthorized person or entity in a manner not permitted under the HIPAA Privacy Rules. A Breach is presumed unless, through a documented risk assessment, a Covered Entity or Business Associate is able to demonstrate that there is a low probability that the Protected Health Information has been compromised. A risk assessment must include at least the following factors:

(i) The nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of reidentification;

(ii) The unauthorized person who used the Protected Health Information or to whom the disclosure was made;

(iii) Whether the Protected Health Information was actually acquired or viewed; and

(iv) The extent to which the risk to the Protected Health Information has been mitigated.

In order to minimize the possibility that a Breach of Unsecured Protected Health Information may occur, the WVHIN has established other policies and procedures requiring the Encryption of Protected Health Information when it is at rest and when it is in motion within its Health Information Exchange. The notification process contemplated by federal and state law applies only if the Breach involves Unsecured Protected Health Information. Unsecured Protected Health Information means that the Protected Health Information has not been rendered unusable, unreadable, or indecipherable by unauthorized individuals or entities through the use of Encryption or other federally-approved technology. If a Breach occurs, but the Breach does not implicate any Unsecured Protected Health Information (the PHI is otherwise secured, i.e. through Encryption or destruction), then no notification is legally required.

Both federal and state laws require a notification to be made if there is a Breach of Unsecured Protected Health Information. As a Business Associate, this notification must be made by the WVHIN to the affected Participating Organization(s). The Participating Organization(s) must then notify the affected Patients directly.

III. PROCEDURES

A. Patient Procedures.

None

B. Participating Organization Procedures.

1. Any Participating Organization which becomes aware of any known Breach involving Unsecured Protected Health Information disclosed through the WVHIN's Health Information Exchange must contact the WVHIN orally and in writing as soon as is reasonably practical, but in no event later than twenty-four (24) hours after discovery. This notification shall include sufficient information to permit the WVHIN to begin its investigation process.

2. A Participating Organization will cooperate with the WVHIN in the WVHIN's investigation of any known unauthorized disclosure of Protected Health Information.

3. Once a Participating Organization has received a written notice from the WVHIN that a Breach of Unsecured Protected Health Information has occurred, the Participating Organization shall determine whether it concurs with the written notification from the WVHIN. If the Participating Organization concurs that a Breach of Unsecured Protected Health Information has occurred, and any risk assessment is unable to demonstrate that there is a low probability that

any affected Protected Health Information has been compromised, then the Participating Organization must notify each Patient or Patients affected by the Breach. This notification should be undertaken without unreasonable delay, but in no event later than sixty (60) days after the date of its discovery.

4. The Participating Organization's notice to Patients must fully comply with the requirements of both the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D, as well as the West Virginia Code at Chapter 46A, Article 2A.

5. The affected Participating Organization or Organizations may require the WVHIN to notify each Patient affected by the Breach if it is determined that the Breach was due solely to a failure of the WVHIN's Health Information Exchange infrastructure or workforce, and was not due to any act or omission of the Participating Organization or Organizations. In order for this delegation of the notification obligation to be effective, all affected Participating Organizations must be in agreement that a Breach has in fact occurred, and that the most appropriate entity to provide the notice to Patients is the WVHIN.

6. Notwithstanding any other provision of this policy, if a law enforcement official informs a Participating Organization that any notification or notice contemplated hereunder would impede a criminal investigation or cause damage to national security, then such notification or notice must be delayed for any and all periods of time authorized by the requirements of both the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D, as well as the West Virginia Code at Chapter 46A, Article 2A.

C. <u>WVHIN Procedures</u>.

1. The WVHIN will maintain an internal incident reporting process designed to identify, internally report, investigate, and resolve known unauthorized disclosures involving Protected Health Information disclosed through the WVHIN's Health Information Exchange. All unauthorized disclosures of Protected Health Information involving the WVHIN will be reported orally and in writing to its Chief Privacy Officer, its Chief Information Officer, or its Chief Operations Officer immediately upon discovery in accordance with West Virginia Health Care Authority Procedure: Response to Unauthorized Disclosures. This report may be originated by a member of the WVHIN Workforce, or by a member of the Workforce of a contractor or Business Associate to the WVHIN.

2. All reports of known unauthorized disclosures will be reported to the State Privacy Office, and will be investigated by the WVHIN's department response team in accordance with Section 3: Procedure as set forth in the Appendix to the West Virginia Executive Branch Procedure: Response to Unauthorized Disclosures, a copy of which is attached hereto and incorporated by reference herein.

3. The WVHIN will report any known use or disclosure of information not provided for by its Business Associate Agreement to any affected Participating Organization. The WVHIN may also ask the affected Participating Organization to assist and otherwise participate in the investigation of the incident under Section 3: Procedure as set forth in the Appendix.

4. After completion of steps outlined in Section 3: Procedure as set forth in the Appendix, the WVHIN must make a determination as to whether a Breach has occurred within the meaning of the HITECH Act, and whether one or more Participating Organizations must be notified.

5. If a Breach within the meaning of the HITECH Act has occurred, the WVHIN will notify any Participating Organization from which the Unsecured Protected Health Information originated. The WVHIN will also develop a plan to mitigate any harm to Participating Organizations and their Patients, to the extent that is practicable.

6. This notice to the Participating Organization must comply with the requirement for Business Associates set forth in the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D. This notification must be undertaken without unreasonable delay and as soon as possible, but in no event later than thirty (30) calendar days after the Breach was initially discovered. The WVHIN will make its staff and the Executive Branch Chief Privacy Officer available to the Participating Organization as a consultative resource.

7. Each Participating Organization that receives written notification from the WVHIN of a Breach of Unsecured Protected Health Information will retain the ultimate authority to determine whether Protected Health Information has been compromised pursuant to the applicable requirements under the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D. In addition, each Participating Organization will retain the ultimate authority to determine whether a Breach under the West Virginia Code at Chapter 46A, Article 2A, is actionable. In making this determination, each Participating Organization may act in accordance with its own policies and procedures, provided that such policies and procedures comply fully with aforementioned federal and state laws and regulations.

8. The WVHIN will also provide notice of the Breach to its Board of Directors without unreasonable delay and as soon as possible, but in no event later than thirty (30) calendar days after the Breach was initially discovered.

9. The WVHIN will notify each Patient affected by the Breach only if requested by the affected Participating Organization(s) based upon a determination that the Breach was due solely to a failure of the WVHIN's Health Information infrastructure or workforce, and was not due to any act or omission of the Participating Organization(s) . In order for this delegation of the notification obligation to be effective, all affected Participating Organizations must be in agreement that a Breach has in fact occurred, and that the most appropriate entity to provide the notice to Patients is the WVHIN.

10. The WVHIN's notice to Patients must fully comply with the requirements of both the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D, as well as the West Virginia Code at Chapter 46A, Article 2A.

11. After any Breach, the WVHIN will undertake a root cause analysis of the circumstances surrounding the underlying Breach, and will determine what organizational or

operational changes in its system, network privacy, network security, Workforce training, policies, and procedures are needed to protect against future Breaches.

12. Any member of the Workforce of the WVHIN, or the Workforce of any contractor to the WVHIN, who was involved or implicated in the Breach may be subject to appropriate sanctions, including possible discharge from employment.

13. Notwithstanding any other provision of this policy, if a law enforcement official informs the WVHIN that any notification or notice contemplated hereunder would impede a criminal investigation or cause damage to national security, then such notification or notice must be delayed for any and all periods of time authorized by the requirements of both the HITECH Act and its implementing regulations at 42 C.F.R. Part 164, Subpart D, as well as the West Virginia Code at Chapter 46A, Article 2A.

Appendix

HIPAA Incident Response

The information contained within this Appendix applies to the West Virginia Executive Branch Procedure: Response to Unauthorized Disclosures.

1.0 BACKGROUND:

A violation of a 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 a privacy 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 HITECH[i], once discovered, an impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach. Breach notification to the individual (to whom the PHI belongs) as well as to the Secretary of the U.S. Department of Health and Human Services (DHHS), is necessary unless, through a documented HIPAA risk assessment, there is a low probability that the PHI has been compromised. Actual notification processes differ based on the number of individuals affected per breach incident. The timeframe for notification begins when a breach is discovered. Note: A breach is considered "discovered" as of the first day it is known to the covered entity or business associate (BA) (or when by exercising reasonable diligence, the issue would have been known to the organization). Additionally, "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.

2.0 POLICY:

Based upon breach risk assessment findings, the covered entity Department will determine if unsecured PHI was breached and follow federal and state laws to report such to the affected individual(s). The State Privacy Office will be responsible for reporting such to the Secretary of DHHS. If a Department is a BA (as defined by HIPAA) of a covered entity, the BA Department is responsible for reporting any breach of unsecured PHI immediately to the covered entity, as well as any reporting required under section 4.1 of the main body of the foregoing procedure.[ii]

3.0 PROCEDURE:

3.1 Covered Entity Department. The Department Privacy Officer will conduct an immediate review to investigate and determine if the information potentially breached was unsecured PHI, and whether or not individual breach notification and mitigation must occur. The Omnibus Rule clarified that any potential breach of PHI is subject to the breach risk assessment required process. The steps listed below should be taken in order to accomplish this objective:

3.1.1 Determine whether the PHI was secured. 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. Note: If the electronic PHI was encrypted according to this Guidance and/or hard copy PHI was appropriately destroyed, individual notification and reporting to the Secretary of DHHS are NOT required. This is known as a "Safe Harbor."

a) If the PHI is considered unsecured, go to Subsection 3.1.2 below.

b) If the PHI was considered secure (in accordance with the above Guidance document and the organization's use of technology), document such in the Department'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 3.4, below.

3.1.2 Determine whether the unsecured 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 BA to another person authorized to access PHI at the same covered entity, BA or affiliated organized health care arrangement.

c) When PHI is improperly disclosed but the covered entity or BA believes in good faith that the recipient of the unauthorized information would not be able to retain the information.

If the unsecured PHI meets one of the exclusions listed above, document such in the Department'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 3.4, below.

3.1.3 If after review, the PHI was considered unsecured, and no exclusion applies, take the following steps to determine the probability that the security or privacy of the PHI was compromised, and is a breach:

a) Begin with the presumption that the incident is a breach, unless the covered entity or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Assess the level (low, medium or high) of probability that the PHI was "compromised," based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

If there is a medium or high probability that the PHI is "compromised," go to subsection 3.1.4, below. If there is a low probability that the PHI is "compromised", document such in your Department'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 3.4, below.

3.1.4 Based on the analysis and resulting findings performed above, the Department Privacy Officer will develop a plan to mitigate the harm, to the extent that this is practicable, and will document the extent to which the risk to the PHI has been mitigated and any other reasonable factors related to the incident. Also follow sections 4.5.8 through 4.5.18 in the foregoing procedure.[iii] Document a final conclusion based on whether or not the final probability that the PHI has been compromised is low, medium or high. If applicable, evaluate what actions the Department requests the BA to take, including covering costs, in accordance with the Business Associate Agreement.

3.1.5 The Department Privacy Officer will notify each affected individual(s) whose information has been inappropriately accessed, acquired or disclosed during such breach. If such breach was caused by a BA, it may be, based on the language within the Business Associate Agreement, the BA's responsibility to perform the following notification steps and to inform the covered entity of such.

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.

b) Once information has been validated, prepare to notify each individual as soon as possible, but within 60 calendar days from discovering the breach. NOTE: All notification materials should be organized and maintained, as the ability for the Department to demonstrate its attempts at notification is an American Recovery and Reinvestment Act of 2009 (ARRA) requirement.

3.1.6 Notification Steps to be followed:

a) Individual Notice Affecting 499 or Fewer Individuals

1. Individual notice must be provided via first class mail at the last known address or email if preferred by the individual (which may have been recorded on the Notice of Privacy Practices Acknowledgement (or other) form).

2. If the individual is deceased, the notice must be sent to the last known address of the next of kin, or personal representative. The 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.

3. If there are 10 or fewer individuals for whom the Department has insufficient or out-of-date contact information to provide the written notice, the 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.

4. If there are 10 or more individuals for whom insufficient or out of date contact information exists, the Department must provide a substitute notice by posting the notice for a period of 90 calendar 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 PHI was involved in the breach.

b) Breaches Affecting 500 or More Individuals

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

2. The 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.

3. Coordinate with the State Privacy Office regarding convening the Privacy Board, as notice to both individuals and to the Secretary of DHHS must occur contemporaneously.

c) If at any point breach notification is deemed not required by this procedure, law or regulations, the Cabinet Secretary or Agency Head has the inherent authority to decide whether or not to voluntarily notify the victim(s) of the incident in order to mitigate effectively any alleged harm and in situations not identified above.

3.2 State Privacy Office. Notice to Secretary of DHHS. In consultation with the appropriate Department Privacy Officer(s) and the Director of Information Security or other Departmental security officer, if appropriate, the State Privacy Office shall determine whether to notify the Secretary of DHHS. This activity shall be known as convening the Privacy Board, and the State Privacy Office will conduct an independent risk assessment to determine whether the PHI has been compromised, based on the factors delineated in 45 CFR § 164.402(2). If the State Privacy Office determines that there has been a breach of unsecured PHI, it shall notify the Secretary electronically:

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

3.2.2 Annually (within 60 calendar days after the close of the previous calendar year) if the breach affects less than 500 individuals. The State Privacy Office may elect to notify the Secretary of DHHS after each breach, thus avoiding additional record keeping and end of year reporting.

3.3 Business Associate Department. Departments functioning as BAs shall notify the appropriate covered entity according to their Business Associate Agreement and in accordance with the HIPAA Privacy Rule, and will follow section 4.0 of the foregoing procedure.[iv]

3.4 Documentation. The allegation, 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 legal counsel, and the documentation will be retained for at least six years.

3.5 Once all steps in the Appendix have been completed, go back to the procedure section 4.5.16 to ensure compliance.[v]

REFERENCE: 45 CFR §§ 164.400 – 414 and § 164.530(f)

---

[i] Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 111-5 and any associated regulations published at 45 CFR parts 160 and 164.

[ii] West Virginia Executive Branch Procedure: Response to Unauthorized Disclosures. Section 4.1.

4.1 Incident Report. All members of the workforce and contractors (on-site vendors) who access state systems, networks and facilities are to immediately report Unauthorized Disclosures (see section 3.2), on the Office of Technology's (OT) website at https://apps.wv.gov/ot/ir/Default.aspx and to their supervisor and/or manager. If the website is not accessible, the workforce member shall call the OT Service Desk at or 1-877-558-9966. 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 The types of PII that were exposed. All actual PII must be redacted or omitted from reports and attachments, including police reports, sent to OT and the State Privacy Office;

4.1.3 How the PII was compromised, including any unauthorized parties that may have accessed the PII;

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

4.1.5 Any other information that may be relevant.

[iii] West Virginia Executive Branch Procedure: Response to Unauthorized Disclosures. Section 4.5.8 – 4.5.18.

4.5.8 Prepare an inventory of exposed data elements.

4.5.9 Using the risk assessment template, analyze possible risks to the affected individuals as a result of the Unauthorized Disclosure. Determine how any risks can be minimized.

4.5.10 If the nature of the incident cannot be fully determined using Department and/or OT resources, contract forensics professionals as needed. See section 4.2.1 (included below) regarding resources available through the cyber insurance carrier.

4.5.11 Notify impacted individuals, if required.

a) Follow W. Va. Code § 46A-2A-101, *et seq.*, concerning breach of the security of a computerized system. Good faith acquisition of PII by a member of the workforce is not a breach, provided that the PII was only used for a lawful purpose and not subject to further Unauthorized Disclosure. Impacted individuals must be notified if:

1. The computerized data elements include a West Virginia resident's first name or first initial and last name linked to the individual's

a. Social Security Number;

b. Driver's license or state-issued ID card number; or

c. Financial account number, credit card or debit card number, in combination with any required security code, access code or password; and

2. The data is

a. Unencrypted or unredacted; and

b. Was or is reasonably believed to have been accessed and acquired by an unauthorized person; and

3. The disclosure causes, or it is reasonably believed that it has caused or will cause, identity theft or other fraud.

b) Determine whether impacted individuals should otherwise be notified because 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.

c) The Cabinet Secretary or Agency Head has inherent authority to use discretion to notify in any other situation not otherwise requiring notification.

d) If notification is required, prepare a list of affected individuals. 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. If the Department does not have sufficient contact information, it may notify individuals through substitute notice as defined within W. Va. Code § 46A-2A101(7) (D). Notification may also be accomplished via email or telephone. Substitute notice may also be appropriate in certain situations. See *Id.*

e) Note: Individual notification may be delayed if a law enforcement agency advises that notification would impede an investigation or security. Obtain this request in writing for the file.

4.5.12 In consultation with legal counsel, identify applicable laws and determine any risks associated with violations of the laws.

4.5.13 If individual notification is required, consider:

a) Developing a notification plan for Department workforce members and issue a statement reminding them to refer all questions to the Department Privacy Officer;

b) Developing a standby statement for media;

c) Creating a communications outline containing:

1. Basic facts (what happened, what data was exposed, to whom);

2. Steps the Department is taking to mitigate harm;

3. Steps the Department is taking to prevent reoccurrence; and

4. An expression of regret and empathy for the situation.

d) Designating a Department leader who will deliver messages and obtain media training if necessary; and,

e) Creating FAQs to support the communications program.

4.5.14 Where individual notification is required, 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) 680-7289
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 a webpage, take calls at an existing phone number, establish a call center, etc.

c) If a call center is authorized, obtain a toll-free number and train personnel on messages.

d) Print and mail letters when authorized. In the few situations when a contracted vendor is visible to the impacted individual(s), Departments may request the vendor take responsibility for notification.

e) Track response, update FAQs, and provide call center training as needed.

4.5.15 Even where individual notification is not required, determine what (if any) individual communications are needed. For example, if members of the workforce 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.

4.5.16 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 appropriate members of the Department's leadership team to facilitate organizational learning.

4.5.17 The Department Privacy Officer is responsible for providing a completed Post Incident Report to the State Privacy Office, Chief Technology Officer and Department Cabinet Secretary within 30 calendar days of the Incident Report. All actual PII must be redacted or omitted from this report and any attachments, including police reports, when submitted to OT and the State Privacy Office. If the Post Incident Report reveals that the incident is a breach and that individual notification was required, the State Privacy Office shall forward the Post Incident Report to BRIM.

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

[iv] *See supra* note ii.
[v] *See supra* note iii, section 4.5.16.

West Virginia Executive Branch Procedure: Response to Unauthorized Disclosures. Section 4.2.1.
BRIM will review the incident report and, if appropriate, coordinate with the cyber insurance carrier. BRIM will advise the Department, State Privacy Office and OT as to resources available through the carrier, such as a breach coach, counsel, public relations expertise, call center services, notification assistance, and forensics.