P3N Policy #7
Data and Privacy Breach Policy

PA eHealth Partnership Program

Subject: P3N Data and Privacy Breach Policy	**Version:** v.4b
Status: Effective January 1, 2024	**Creator:** Kay Shaffer
Approval Date: October 4, 2023	**Contact:** Kay Shaffer (kashaffer@pa.gov)
Original Issue Date: April 13, 2015	**Last Review Date:** October 4, 2023
Related Documents:	-Terms and Definitions -Pennsylvania eHealth Partnership Program Uniform Participant Agreement v.4c

1. **PURPOSE.** This document establishes the policy for communicating, managing and reporting on Data and Privacy Breaches.

2. **SCOPE.** This document applies to the Pennsylvania Department of Human Services eHealth Partnership Program (PA eHealth) and all Certified Participants (CPs) in the Pennsylvania Patient & Provider Network (P3N).

   2.1. This policy is intended to be consistent with and does not replace or supersede any federal regulations or laws (such as Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH)) or state privacy and security laws and regulations.

   2.2. For purposes of this policy, a reportable breach is one which is known or suspected to involve the P3N infrastructure or any of its CPs as a result of their participation in the P3N. Breaches that impact CPs independent of the P3N are not subject to this policy.

3. **OBJECTIVES.** The objective of this policy is to:

   3.1. Establish the requirements for Breach notification and reporting.

   3.2. Define the responsibilities for Breach handling.

   3.3. Define the possible consequences for Data and Privacy Breaches.

   3.4. Establish the reconsiderations available for any Breach consequences.

4. POLICY

4.1. General

4.1.1. CPs shall provide PA eHealth with appropriate points of contact for Breach notification and shall promptly notify PA eHealth if those points of contact change.

4.1.2. PA eHealth shall maintain a list of CP contacts for Breach notification purposes.

4.1.3. CPs are accountable for maintaining and adhering to policies and procedures within their respective organizations to notify appropriate individuals regarding Breaches relative to the P3N.

4.1.4. A Breach of Protected Health Information (PHI) shall be treated as "discovered" as of the first day on which such Breach is known to the CP, or, if by exercising reasonable diligence should have been known to the CP.

4.1.5. Each CP and its MOs have the obligation to identify, notify, investigate and mitigate any known Breach or potential Breach, and when detection of a reportable Breach through the P3N has occurred, the CP will notify PA eHealth and PA eHealth will notify the P3N vendor and any affected CPs of the reportable Breach in accordance with these procedures.

4.1.6. Notwithstanding anything to the contrary, the CP and its MOs are required to comply with applicable federal and state laws with regard to Covered Entities and their Business Associates as to providing notification of a reportable Breach of PHI.

4.1.7. CP shall communicate with affected parties in compliance with federal and state law to conduct appropriate analysis and investigation of a potential or suspected privacy violation or security Breach.

4.2. Breach Notification

4.2.1. As soon as reasonably practicable, but no later than twenty-four (24) hours after confirming that a Breach involving the P3N has occurred, the CP will:

4.2.1.1. Notify PA eHealth that the Breach occurred by sending a secure email or by phone call to PA eHealth.

4.2.1.2. PA eHealth will send a notification of determination as to the Breach to other CPs who are likely impacted by the Breach. Notifications sent to other CPs will be sent to the Breach notification contact list.

4.2.2. CP will include in its notification sufficient information for PA eHealth and other likely impacted CPs to understand the nature of the Breach. Such

notification should include, to the extent available at the time of the notification, the following information:

4.2.2.1. Brief description of the Breach, including the date of discovery and location of the Breach

4.2.2.2. Description of the roles of the people involved in the Breach (e.g. employees, Authorized Users, etc.), including any third-party services which may be involved in breach investigation and response

4.2.2.3. The type of PHI Breached (such as full name, social security number, date of birth, etc.)

4.2.2.4. CPs likely impacted by the Breach

4.2.2.5. Number of individuals or records impacted or estimated to be impacted by the Breach

4.2.2.6. A description of what the CP involved is doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches. Include the name of the contact person for this incident.

4.2.2.7. Current status of the Breach (under investigation, contained or resolved)

4.2.2.8. Corrective action taken and steps planned to be taken to prevent a similar Breach

4.2.3. The notification shall not include any PHI. CPs shall label the notification as Confidential CP Information. All information disclosed by the CP shall be treated as confidential by PA eHealth and other CPs, to the extent possible, until the information is publicly disclosed by the Breaching CP.

4.2.4. The CP shall have a duty to supplement the information contained in the notification as it becomes available.

4.2.5. If, on the basis of the information that the CP has, the CP believes that it should temporarily cease exchanging Data through the P3N, it may request a voluntary suspension of its P3N Services in accordance with this policy and Section 7 Suspension and Termination of Agreements in the Pennsylvania eHealth Partnership Program Uniform Participant Agreement (PAR).

4.2.6. PA eHealth will provide notice to the affected CP(s) of a P3N Breach identified by PA eHealth, for Breaches that occurred under the operational control of PA eHealth, following the same process as outlined in this Section 4.2.

4.3. **Health Information Exchange Trust Community Committee (HIETCC) Engagement in the Disposition of Breach Notifications**

4.3.1. At the earliest possible time, PA eHealth shall schedule a meeting of the HIETCC upon receipt of the Breach notification for the purpose of reviewing the notification and determining the following:

4.3.1.1. The impact of the Breach on the privacy, security and integrity of PHI exchanged through the P3N;

4.3.1.2. Whether PA eHealth needs to take any action to suspend the CP(s) or MO(s) involved in the Breach in accordance with the PAR and this policy;

4.3.1.3. Whether other CPs that have not been notified of the Breach would benefit from a summary of the notification; or whether a summary of the notification to the other CPs would enhance the security of the P3N; and,

4.3.1.3.1. If PA eHealth determines that a summary should be distributed to CPs, PA eHealth will distribute such summary in a timely manner.

4.3.1.3.2. This summary shall not identify any of the CPs or individuals involved in the Breach.

4.3.1.4. Whether PA eHealth should take any other measures in response to the notification.

4.3.2. PA eHealth and the HIETCC are permitted to request additional information from the CP(s) or MO(s) involved in the Breach.

4.3.3. Once sufficient information about the Breach becomes available, the HIETCC will meet at the earliest possible time to advise as to whether the actions taken by the CP(s) or MO(s) involved in the Breach are adequate to mitigate the Breach and prevent a similar Breach from occurring in the future. Once the HIETCC is satisfied that the CP(s) or MO(s) have taken all appropriate measures, the HIETCC will advise that the Breach is resolved. CPs will update and inform PA eHealth as soon as possible regarding new information involving the Breach.

4.3.4. This resolution will be communicated to PA eHealth and all CPs as applicable.

4.4. **Breach Reporting**

4.4.1. CP shall provide a full report of a confirmed reportable Breach involving the P3N, that occurred under the operational control of the CP or its MO(s), to PA eHealth without unreasonable delay and no later than 30 days from the discovery of the Breach; including, to the extent possible, the information listed in Section 4.2.2. above and any additional information required to be provided by the CP in its notification to affected individual(s).

4.4.1.1. If the CP can discern what PHI traveled over the P3N, then it may limit what Breaches it reports to PA eHealth to such information. However, if the CP does not have the means to identify if the Breached PHI traveled over the P3N or not, then it must report all Breaches to PA eHealth as stated in 4.4.1 above.

4.4.2. CP shall provide written reports through secure email, the U.S. Postal Service, or a commercial delivery service that provides a receipt.

4.4.3. As part of its annual report to the Governor, the President pro tempore of the PA Senate and the Speaker of the PA House of Representatives PA eHealth will include a summary of reportable security Breaches involving the P3N that occurred and corrective actions that were taken.

4.5. **Privacy Violations, Breach Report Handling, and Possible Consequences**

4.5.1. CP shall have policies to address appropriate actions taken in response to a Breach or other privacy violation consistent with federal and state laws.

4.5.2. CP should follow and enforce its own institution's confidentiality policies and disciplinary procedures, relating to confidentiality and breach reporting.

4.5.3. CP shall train their workforce members in its policies in compliance with federal and state laws.

4.5.4. PA eHealth shall report all Breaches involving the P3N to the Secretary of DHS or designee and shall apprise the HIETCC of any such breaches within one hour of a suspected breach and within 24 hours of a confirmed breach.

4.5.4.1. PA eHealth may make determinations regarding actions, sanctions, policy changes, procedure changes, or terminations based on Breach information.

4.5.4.2. The HIETCC may make recommendations to PA eHealth regarding actions, sanctions, policy changes, procedure changes, or terminations based on Breach information.

4.5.5. In the event of a Breach determined by PA eHealth as posing possible ongoing harm to the P3N without report of an associated solution, PA eHealth may decide that the CP involved be temporarily suspended from the P3N for up to five (5) business days while investigations and remediation is carried out.

4.5.5.1. The CP recommended for temporary suspension shall be afforded the opportunity to communicate with PA eHealth prior to temporary suspension.

4.5.5.2. The CP shall have the opportunity to alleviate the harmful actions before temporary suspension.

4.5.6. If the action(s) that may cause the P3N harm cease or the investigation of the Breach cause is completed prior to the expiration of the temporary suspension, then PA eHealth may recommend an early reconnection of the CP.

4.5.7. If the investigation requires more than five (5) business days, PA eHealth may continue the temporary suspension pending completion of the investigation.

4.5.8. Based on the findings of the investigation and the possible impact to the P3N and its trust community, PA eHealth may require additional sanctions by the CP or the MO through the CP. Examples of the types of sanctions that may be required include, but are not limited to:

4.5.8.1. If not already developed, requirement for the creation of a corrective action plan and schedule, including sufficient related reporting to allow the Authority to monitor progress and compliance by the CP. PA eHealth may suspend the CP for the time necessary to generate or enact the corrective action plan.

4.5.8.2. Establishment of a probationary period for full use of the P3N in the manner in which it was previously used. During this probationary period, PA eHealth shall work with the CP so that the CP's corrective action plan is proceeding on schedule.

4.5.8.3. An extended period of full suspension from the P3N (e.g., several months). During this suspension period, PA eHealth shall work with the CP to ensure that the CP's corrective action plan is proceeding on schedule.

4.5.8.4. In the case of failing to abide by the corrective action plan or by terms accompanying any probationary period or suspension imposed by PA eHealth, PA eHealth will terminate the CP's use of the P3N.

4.5.8.5. PA eHealth will immediately terminate Access to the P3N based on a finding of an egregious violation or a confirmed violation of HIPAA, or some other federal or state law.

4.5.9. If PA eHealth determines that an MO poses a risk for continued Breaches and/or security problems, then PA eHealth may sanction the MO. Sanctions may take any of the forms listed under 4.5.8. The CP to which the MO belongs must cooperate in enacting the sanction. If the CP does not cooperate with carrying out the sanction, PA eHealth may consider sanctioning the CP.

4.5.10. PA eHealth or the DHS Privacy Officer shall inform the sanctioned CP and/or MO(s) by letter via a method allowable under Section 34 of the PAR.

4.5.10.1. PA eHealth shall include in the letter regarding the sanction the terms and duration of the sanction, as well as any rights the recipient of the sanction may have to submit a request for reconsideration to PA eHealth (see section 4.6).

4.5.11. PA eHealth shall follow all federal and state laws regarding reporting of legal violations to federal and state authorities and shall cooperate with federal and state authorities for any investigation that such authorities may initiate.

4.6. **Reconsiderations**

4.6.1. If PA eHealth imposes sanctions on a CP or MO(s) that suspends, restricts, or terminates access to or use of the P3N, such CP and MO(s) shall be afforded an opportunity to request that PA eHealth reconsider its decision.

4.6.1.1. The CP or MO must submit its request for reconsideration by written letter to PA eHealth within seven (7) business days of receipt of the official sanction notice, care of the Director of PA eHealth, and state the specific reasons and information supporting why PA eHealth should reconsider the sanction it imposed on the CP or MO ("requestor.") The request must be sent via a method allowable under Section 34 of the PAR.

4.6.1.2. The "reconsideration period" shall commence upon the first business day of receipt of the requestor's written letter and a final decision rendered as quickly as possible, but in no case more than twenty (20) business days after receipt.

4.6.2. During the reconsideration period:

4.6.2.1. PA eHealth may request an in-person meeting with the requestor or between the requestor, the HIETCC and/or PA eHealth in order to obtain further information as needed.

4.6.2.2. The sanction imposed by PA eHealth upon the requestor shall continue in full force and effect up to and until the reconsideration period has ended or a reconsideration decision has been made.

4.6.3. By the end of the reconsideration period, PA eHealth shall render a final reconsideration decision to continue or end the previously imposed sanction.