# P3N Policy #6
# Auditing Policy

## PA eHealth Partnership Program

| | |
|---|---|
| **Subject:** P3N Auditing Policy | **Version:** v.4b |
| **Status:** Effective January 1, 2024 | **Creator:** Kay Shaffer |
| **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<br>-Pennsylvania eHealth Partnership Program Uniform Participant Agreement v.4c |

1. **PURPOSE.** This document establishes a policy to ensure that appropriate auditing, logging, and monitoring policies are in place and adhered to.

2. **SCOPE.**

   2.1. This document applies to all Certified Participants (CPs) in the Pennsylvania Patient & Provider Network (P3N).

   2.2. 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.

   2.3. This policy is not intended to address access subsequent to Protected Health Information (PHI) being acquired through the P3N. For example, once the information becomes part of an MO's record, it is the MO's responsibility to account for compliant access and disclosure.

   2.4. The scope is limited to PHI that travels over the P3N.

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

   3.1. Establish PA eHealth's right to conduct, or to have conducted by a third party, Audits of P3N Usage and security.

   3.2. Define Auditable events and information to be contained in Audit logs.

   3.3. Define policies for the maintenance of Audit Files and Audit Trails.

   3.4. Define polices related to Accounting of Disclosures.

4. **POLICY**

4.1. **PA eHealth Auditing**

4.1.1. PA eHealth may conduct random and scheduled Audits of P3N Usage. Any on-site audits would be scheduled so as not to negatively impact the CP.

4.1.2. PA eHealth may contract for the services of a certified third-party auditor to conduct random or scheduled external Audit of P3N Usage and security practices.

4.2. **CP Audit Logs and Auditable Events**

4.2.1. Regarding exchange of data through the P3N, all transactions made by CP and its MOs shall be identified by a unique record key or number, which shall be contained within an audit log.

4.2.2. CPs shall record the following information in relation to logging on and off of the system their staff uses to Access the P3N, and shall obligate their MOs to record the same as a condition of participation:

4.2.2.1. User Identification – unique identification of the Authorized User of the system.

4.2.2.2. Date and System Time – the exact date and time of the Access event and the exit event.

4.2.2.3. Access Device (optional) – terminal or work station or device from which the Authorized User obtained Access.

4.2.2.4. User's Role (optional) – if the system uses role-based Access to determine permissions for users, then the Authorized User's assigned role should be logged.

4.2.3. CPs shall monitor Access and Use of PHI, either directly or through MOs, obtained through the P3N on its behalf for the purpose of detecting unauthorized Access or Use, and shall notify PA eHealth of any such unauthorized Access or Use.

4.2.4. CP and its MO shall review Audit logs and have policies and procedures for addressing unauthorized Access or Use.

4.2.5. CP Audit Files shall include entries at the time events occur on their systems related to PHI such as Create, Modify, View, and Delete.

4.2.6. Where technically feasible, all Audit File entries made by CP and/or its MOs, triggered by events such as those listed in 4.2.5 shall include the following information:

4.2.6.1. User Identification – unique identification of the Authorized User of the system.

4.2.6.2. Date and System Time – the exact date and time of the Access event and the exit event.

4.2.6.3. Patient Identification – unique identification of the patient to distinguish the patient and the connected PHI.

4.2.6.4. Access Device (optional) – terminal or workstation or device from which the Authorized User obtained Access.

4.2.6.5. Type of Action – as identified in the list under 4.2.5.

4.2.6.6. Identification of the Patient Data Accessed– if it is possible to identify the information that was Accessed, it should be recorded. Additionally or alternatively, the specific category of Data is useful, such as demographics, pharmacy Data, test results, and transcribed notes, etc.

4.2.6.7. Source of Access (optional unless the trail is combined from multiple systems or can be indisputably inferred) – the identification of the application through which the Access occurred.

4.2.6.8. User's Role (optional) – if the system uses role-based Access to assign permissions for Authorized Users, then the Authorized User's role should be logged. This will help to determine if that Authorized User should have been performing the event that triggered the recording.

4.3. **Maintenance of Audit Files and Audit Trails**

4.3.1. Restricted access to Audit Files and Audit Trails shall be maintained by the CP and its MOs at all times. Only authorized personnel shall access Audit Files or Audit Trails.

4.3.2. CPs and MOs must have Audit Files and Audit Trails that are created automatically without the need for manual intervention.

4.3.3. CP and its MOs shall not allow or have the ability to modify Audit Files.

4.3.4. CPs and MOs will retain Audit Files for a period of seven (7) years.

4.4. **Authority Audits of CPs**

4.4.1. PA eHealth shall Audit a CP no more frequently than biennially, unless a security breach resulting in the exposure of patient PHI warrants investigation.

4.4.2. When conducting Audits of a CP, PA eHealth will attempt to limit its requests to only those Audit Files and Audit Trails containing information about PHI that traveled over the P3N. However, if a CP cannot identify what PHI in its system(s) traveled over the P3N, PA eHealth may request Audit Files and

Audit Trails of any systems that might contain PHI that traveled over the P3N.

4.5. **Patient Auditing and Accounting of Disclosure**

4.5.1. CP shall adhere to 45 CFR §164.528.

4.5.2. CP shall advise its MOs of its obligations under 45 CFR §164.528.

4.5.3. Patients requesting Access to, correction, amendment of, or accounting of Disclosures of Data, will be referred back to the Privacy Office of the appropriate CP or MO.

4.5.4. CPs shall cooperate in good faith, and as appropriate, with requests from other CPs regarding privacy issues.