P3N Policy #4
User Management Policy

PA eHealth Partnership Program

Subject: P3N User Management 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.4d

1. **PURPOSE.** This policy establishes minimum standards and requirements for Authorized User management, including User Authentication, User Authorization and Access Controls, set forth for the Certified Participants (CPs) in the Pennsylvania Patient & Provider Network (P3N) to maintain an appropriate level of security to avoid unauthorized Access to and Disclosure of Protected Health Information (PHI) through the P3N.

2. **SCOPE**. This document applies to all CPs connected to the 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.

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

   3.1. Define the minimum standards and requirements of the P3N CPs to establish:

      3.1.1. Procedures for the authentication of users of the P3N

      3.1.2. Requirements for Access Controls and user account maintenance

      3.1.3. User roles and requirements for the authorization of users of the P3N

   3.2. Assign responsibility to the Pennsylvania Department of Human Services eHealth Partnership Program (PA eHealth) to facilitate awareness and compliance with this policy.

4. **POLICY**

   4.1. **User Authentication**

      4.1.1. All CPs shall implement and enforce a User Authentication mechanism that meets legal requirements, including at a minimum:

4.1.1.1. CPs must authenticate, either directly or through their MOs, each Authorized User's identity prior to providing any user with Access to PHI through the P3N or CPs' Health Information Exchange (HIE) systems.

4.1.1.2. PA eHealth and CPs may deny Access to the P3N to an individual or MO for cause where violations of law or PA eHealth policies are known.

4.2. **Access Controls**

4.2.1. CPs are required to protect electronic PHI exchanged through, created or maintained by the P3N technology through the implementation of appropriate technical, physical, and administrative safeguards, as set forth in the HIPAA Security Rules.

4.2.2. In order to gain access to the P3N, Authorized Users must provide unique User Authentication. At PA eHealth's request, the CP shall provide a detailed description of the Access Controls that enable their Authorized Users to access the P3N.

4.2.3. The use of another Authorized User's credentials to Access the P3N is prohibited and generic or shared IDs are not allowed.

4.2.4. Authorized Users are responsible for all activities related to their unique credentials.

4.3. **Training**

4.3.1. The CP shall provide or arrange for training as appropriate in the Use of the P3N and the requirements of the Pennsylvania eHealth Partnership Program Uniform Participant Agreement (PAR) for all the CP's Authorized Users.

4.3.2. This training should be consistent with any Documentation that may be provided by PA eHealth regarding Use of the P3N.

4.4. **P3N Site Administrator**

4.4.1. The CP shall designate a single individual who shall be responsible for managing communications between the CP and PA eHealth in connection with the CP's participation in the P3N.

4.4.2. A CP Site Administrator shall be responsible for adding, deleting and maintaining the user level of Authorized Users' along with their access keys (user names and passwords) for using the P3N as outlined in this policy.

4.4.3. In the absence of an architecture where a central Site Administrator is assigned this responsibility, the CP must have appropriate processes or policies in place where this responsibility is delegated to an MO.

4.5. Wind Down Responsibilities

4.5.1. The CP is strongly encouraged to have plans in place for supporting its MOs in the case the CP chooses to terminate this Agreement and its Access to the P3N Services.

4.5.2. Such plans should include proper notification to its MOs, and reasonable and appropriate assistance for transitioning to another CP as applicable.