P3N Policy #10
Security Policy

PA eHealth Partnership Program

Subject: P3N Security 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: September 5, 2018	**Last Review Date:** October 4, 2023
Related Documents:	-P3N Application For Participation v.4c -Certification Policy and Process -Pennsylvania eHealth Partnership Program Uniform Participant Agreement v.4c

1. **PURPOSE.** This policy establishes the minimum-security requirements and responsibilities for Certified Participants and Provisionally Certified Participants, collectively referred to as "Participants", to join and participate in the Pennsylvania Patient and Provider Network (P3N).

2. **SCOPE**. This document applies to all Participants connected to the Pennsylvania Patient and Provider Network (P3N) and their associate workforce and is applicable to all services defined in the PAR.

   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. Establish baseline security measures required as part of P3N participation to ensure patient confidentiality and data security.

   3.2. Minimize the risk of security incident or data breach due to insufficient security controls.

4. POLICY

4.1. General

4.1.1 The P3N Security Policy is governed by P3N Policy #2 – Documentation Change Management.

4.1.2 The P3N Health Information Exchange Trust Community Committee (HIETCC) will make recommendations for proposed policy and procedure changes and will collaborate with the PA eHealth Partnership to finalize proposed changes.

4.1.3 Participants shall be compliant with all P3N Security Policy guidelines. If Participants are not found to be in compliance with all applicable P3N Security policies and guidelines, they will have exactly one (1) year from the date of signing the P3N Participation Agreement to demonstrate full compliance.

4.2 Duties and Responsibilities

4.2.1 Participants shall store all PHI and confidential data only in secure data facilities located in the United States.

4.2.2 Participants shall ensure that any agent, including a subcontractor, to whom it provides PHI, will comply with this Security Policy and HIPAA.

4.2.3 Participants shall report any security incident of which Participant becomes aware to PA eHealth. For purposes of this Policy, "Security Incident" shall mean the attempted or successful unauthorized access, Use, Disclosure, modification or destruction of PHI originating from the Participant or interference with system operations in an information system.

4.2.4 Participants shall maintain in full force and effect Cyber Liability insurance, including coverage for Network Security and Privacy Breach as defined in the PAR.

4.2.5 Participants shall provide annually to P3N proof of security certification/accreditation which includes a copy of their current HITRUST Common Security Framework (CSF) certification, National Institute of Science and Technology (NIST) Cybersecurity Framework average score of 2.5 or higher, Electronic Healthcare Network Accreditation Commission (EHNAC) Health Information Exchange Program (HIEP) accreditation or certification/accreditation by a nationally recognized third party security certification program that meets standards similar to HITRUST, NIST, and EHNAC.

4.2.5.1 Proof of security certification/accreditation may include:

4.2.5.1.1. Certification Letter relating to the Providers' sites, systems, software, operations, and procedures that are directly related to the use of services provided through P3N.

4.2.5.1.2 Un-redacted or redacted report, including findings and corrective action plans relating to the Providers' sites, systems, software, operations, and procedures that are directly related to the use of services provided through the P3N. Participants may redact from the report any confidential or business-sensitive information not directly related to services provided through P3N.

4.2.5.2 Participants must achieve, or be actively working on achieving, security certification/accreditation at the time of signing the P3N Participation Agreement.

4.2.5.2.1 Participants must achieve security certification/accreditation within two (2) years of signing the P3N Participation Agreement.

4.2.5.2.2 Participants may request an extension of six (6) months to obtain certification one (1) time.

4.2.5.2.2 PA eHealth Partnership may grant a six (6) month extension at its discretion as long as the Participant is working in good faith to obtain security certification/accreditation. If PA eHealth Partnership believes the Participant is not working in good faith to obtain security certification/accreditation, the Participant will not be provided the extension.

4.2.5.3 Participants that have not yet achieved security certification/accreditation shall provide annually to P3N a copy of their HIPAA security audit un-redacted or redacted report, including findings and corrective action plans relating to the Participant’s sites, systems, software, operations, and procedures that are directly related to the use of services provided through the P3N. Participants may redact from the report any confidential or business-sensitive information not directly related to services provided through P3N.

4.2.5.3.1 HIPAA security audits shall be performed by independent, qualified organizations to ensure appropriate technical, physical, and administrative safeguards are in place.

4.2.5.3.2 HIPAA security audits must have been completed within 12 months of initial P3N Certification or annual P3N Certification renewal.