Central PA Connect
HEALTH INFORMATION | EXCHANGE

Policy Title:	Data Provider and Data Recipient Policy				
Effective Date:	5/14/19	Revision Date:	12/22/2025	Review Date:	12/22/2025
Policy Owner:	Marianne Smith				
Policy Approver:	Keith Cromwell				

POLICY PURPOSE:
This policy addresses data management and use.

POLICY STATEMENT:
This Policy in conjunction with the following UPHS Policies collectively detail the requirements for data management and use by a Central PA Connect Member Organization:

- Access Controls for Information Assets
- University of Pennsylvania Health System Disclosure of PHI with Patient Authorization
- Hospital Acceptable Use of Electronic Resources
- University of Pennsylvania Health System Breach Notification Policy

APPLICABILITY/SCOPE/EXCLUSION:
The policy is applicable to all Central PA Connect Member Organizations and any individual designated to use the services. Policy covers data provider requirements, data recipient uses, restrictions and required consents.

DEFINITIONS:
Data Provider: means a Member Organization that provides patient data to the CPC-HIE.

Data Recipient: means a Member Organization that receives or accesses patient data from the CPC-HIE.

Member Organization (MO): means individuals and entities (including, but not limited to, Health Care Providers, physician practices health care facilities, medical laboratories, payers, etc.) that enroll in and connect to CPC-HIE to send and/or receive health information.

Patient: means any person for whom the Member Organization is a custodian for patient data.

Patient Data: means health information that is created or received by a Member Organization and relates to past, present, or future physical, social or mental health of an individual or the provision of health care to an individual that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, including such information that is made available for exchange by a data provider. Patient Data includes Protected Health Information and Super Protected Data.

Protected Health Information (PHI): shall have the meaning given in 45 CFR § 160.103 and includes Electronic PHI.

Super Protected Data: means Protected Health Information that, under Applicable Law, requires a higher level of consent for Use and Disclosure, including HIV-related information, under 35 P.S. § 7607 (also known as Act 148) and its implementing regulations, mental health treatment information under the Pennsylvania Mental Health Procedures Act, 50 P.S. §§ 7107-7116, and its implementing regulations set forth at 55 Pa. Code. § 5100, et seq., and the Pennsylvania Drug and Alcohol Control Act, 71 P.S. § 1690.108(c) and its implementing regulations at 4 Pa. Code § 255.5, et seq., as well as federal law and regulations governing the Confidentiality of Substance Abuse Disorder Patient Records, set forth at 42 U.S.C. § 290dd-2 and 42 C.F.R. Part 2.

PROCEDURE:
Member Organizations shall provide access to Protected Health Information. MO providing data shall use best efforts based upon industry standards to ensure that accurate and complete patient matching occurs in their system and that such data is available to Central PA Connect for management of the CPC-HIE master patient index. Each data provider shall use reasonable and appropriate efforts to assure that all Protected Health Information it provides to the CPC-HIE is accurate, free from serious error and reasonably complete. Data recipients may access and use patient data for treatment, payment, and health care operations.

Members are responsible for data protection. This includes:

- Protecting all shared information using strong safeguards, including encryption for data at rest and in transit, ensuring only those with the correct decryption key can access the information.
- Enforcing strict access controls by assigning roles and permissions so that only properly authorized individuals can view or handle the data.
- Securing and promptly disposing of data once it is no longer required.
- Provide regular security training for staff involved in data sharing processes.

PROHIBITED ACTIVITIES:
Data Provider shall not knowingly or negligently allow any information to be transmitted that violates the proprietary rights, privacy rights, or any other rights of a third party, including any patient.
Data Recipient may not use or permit the use of patient data for any purpose or use other than for the permitted uses noted above or in any manner prohibited by HIPAA or other applicable law, including the laws related to Super Protected Data.

REVIEW AND VIOLATIONS: N/A

ROLES AND RESPONSIBILITIES: N/A

APPENDICES: N/A

FORMS: N/A

REFERENCES: N/A

- Access Controls for Information Assets
- University of Pennsylvania Health System Disclosure of PHI with Patient Authorization
- Hospital Acceptable Use of Electronic Resources
- University of Pennsylvania Health System Breach Notification