Central PA Connect
HEALTH INFORMATION | EXCHANGE

Policy Title:	Adverse Security Event Reporting				
Effective Date:	8/1/2020	Revision Date:	4/1/2025	Review Date:	4/1/2025
Policy Owner:	Marianne Smith				
Policy Approver:	Keith Cromwell				

POLICY PURPOSE:
This policy summarizes Central PA Connect process for dealing with adverse security event reporting.

POLICY STATEMENT:
This policy in conjunction with the following policies collectively detail the requirements for Adverse Security Reporting within Central PA Connect HIE:

- 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 provided by Central PA Connect HIE.

DEFINITIONS:

Adverse Security Event (ASE) The unauthorized acquisition, access, disclosure, or use of individually identifiable health information (as defined in the HIPAA Regulations) while such information is being transmitted between member organizations and Central PA Connect HIE and any of its connected parties, including but not limited to, Pennsylvania Patient & Provider Network (P3N) Connections, Carequality, and eHealth Exchange pursuant to a valid CCD, but shall not include (i) any unauthorized acquisition, access, disclosure or use of encrypted data; (ii) any unintentional acquisition, access, disclosure, or use of health information if (I) such acquisition, access, disclosure, or use was made in good faith and within the course and scope of the employment, or other professional relationship if not an employee, of an End User; and (II) such health information is not further acquired, accessed, disclosed or used by the End User.

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.

PROCEDURE:
If a Member Organization becomes aware of a potential Adverse Security Event (ASE), their designed security individual must report the event within 24 hours to Central PA Connect (CPC) and any other CPC HIE member organizations whose health data has been breached.

As soon as reasonably practicable, but not later than 6 hours after determining that an ASE has occurred, the member organization shall notify CPC HIE and all CPC HIE member organizations that are likely impacted by the ASE, of such ASE. The notification should include sufficient information for CPC HIE and other member organizations to understand the nature of the ASE. The notification should include:

- Detailed description of the ASE (including date/time of occurrence)
- Description of the roles of the individuals involved in the ASE
- Type of health data that was exposed as part of the ASE
- The other member organizations likely impacted by the ASE
- Number of individual records impacted (or estimated to be impacted) by the ASE
- Actions taken by the member organization to mitigate the ASE
- Corrective action steps taken or planned to prevent a similar ASE in the future

The MO shall supplement the information contained in the ASE notification as it becomes available and cooperate with other CPC HIE MOs and CPC HIE in performing such actions as are required and as are necessary to mitigate the harmful effect of the ASE.

Upon notification of an ASE, the CPC HIE Product Manager in conjunction with the CPC compliance staff will research the reported event to determine if it qualifies as an ASE. If it is determined that an ASE has occurred, notifications will be made as outlined in the University of Pennsylvania Health System Breach Notification Policy to the appropriate parties, including but not limited to HHS, the patients, and 3rd Party networks (Pennsylvania Patient and Provider Network, eHealth Exchange, Carequality, etc).

Carequality Specific Reporting

As soon as reasonably practicable, but not later than 5 business days after determining that an ASE has occurred, CPC HIE will notify Carequality of the ASE. If the ASE occurs between CPCHIE and a federal agency, the reporting will occur within 24 hours of determination. The notification should include sufficient information for Carequality to understand the nature of the ASE. The notification should include:

- Detailed description of the ASE (including date/time of occurrence)
- Description of the roles of the individuals involved in the ASE
- Type of health data that was exposed as part of the ASE
- The other member organizations likely impacted by the ASE
- Number of individual records impacted (or estimated to be impacted) by the ASE
- Actions taken by the member organization to mitigate the ASE
- Corrective action steps taken or planned to prevent a similar ASE in the future.

PROHIBITED ACTIVITIES: N/A

REVIEW AND VIOLATIONS:

The MO will routinely monitor their system to identify if any unauthorized access has occurred and will report those violations to the CPC HIE Product Manager as outlined above.

ROLES AND RESPONSIBILITIES:

Member Organizations will be responsible for reporting any potential ASEs to Central PA Connect HIE.

Central PA Connect HIE will be responsible for researching the potential ASE and will report all confirmed ASEs to the appropriate parties.

APPENDICES: N/A

FORMS: N/A

REFERENCES:
University of Pennsylvania Health System Breach Notification Policy