1801 Market Street, Suite 750 Philadelphia PA, 19103 www.healthshareexchange.org

Data Misuse Policy

Version	Approval Date	Owner
1.1	November 8, 2018	Privacy Officer

1. Purpose

The purpose of HealthShare Exchange (HSX) Data Misuse Policy is to outline the appropriate response to a potential or actual misuse of Data and the plan of action for investigation and response.

2. Scope

Data Misuse shall mean the unauthorized acquisition, access, use or disclosure of Data by a Participant or Authorized User in a manner inconsistent with the Use Cases, the Permitted Purposes and/or the HSX Policies. The term "Data Misuse" does not include a Breach or Security Incident described in the Business Associate Agreement (BAA). Any Data Misuse that is also a Breach or Security Incident shall be governed solely by the provisions in the HIPAA BAA which pertain to Breaches and Security Incidents.

Participant shall mean a person or entity that has entered into a binding agreement with HSX setting forth the terms and conditions of access to and use of the HSX Network after such person or entity is approved as an authorized Participant of HSX.

Authorized User shall mean an individual who is also a registered Participant, or an individual designated by a Participant to use the Services on behalf of an approved and authorized Participant.

3. Policy

Data Misuse Notification

- Data Misuse Notification. As soon as reasonably practicable, but no later than twenty-four (24) hours after obtaining knowledge that a potential or actual Data Misuse has occurred, Participant shall notify HSX and the Participant which is the subject of the potential or actual Data Misuse of such potential or actual Data Misuse. This notification may be initially provided to HSX and the subject Participant by telephone

but must be followed up in writing to HSX and the subject Participant within twenty-four (24) hours after telephone notification is made ("Data Misuse Notification") and shall include sufficient information for HSX and the subject Participant to understand the nature of the potential or actual Data Misuse. For instance, such Data Misuse Notification could include, to the extent available at the time of the notification, the following information:

- One or two sentence description of the Data Misuse including the Participant and/or Authorized User involved in the potential or actual Data Misuse;
- Description of the roles of the persons or entities involved in the Data Misuse (e.g., employees, parties, service providers, unauthorized persons, etc.), if known;
- The type of Data that was, or has the potential to be, misused and the Use Case, Permitted Purposes and/or HSX Policies affected;
- Other Participants likely impacted by the Data Misuse, if known;
- Number of individuals or records impacted/estimated to be impacted by the Data Misuse;
- Actions taken by the notifying Participant to mitigate the Data Misuse, if any; and
- Current status of the Data Misuse (under investigation or resolved).

4. Procedures

- **Investigation**. As soon as possible after receipt of the Data Misuse Notification, HSX and/or its representatives shall commence an investigation into the allegations contained in the Data Misuse Notification which shall include but not be limited to an interview with representatives of the affected Participants, the provision of notice to each affected Participant of their duty to present Supplemental Data Misuse Information, and the consideration of such Supplemental Data Misuse Information and other information, if any. HSX shall issue its written report, which shall include its recommendations, to the HSX Board with copies to the affected Participants within five (5) business days after it its investigation is completed.

- **Supplemental Data Misuse Information.** At all stages in the process, Participants disclosing, reporting and/or responsible for the potential or actual Data Misuse shall have a duty to supplement the information contained in the Data Misuse Notification as it becomes available, produce information including audit logs that would be applicable to the investigation and cooperate with the other Participants and HSX and its representatives ("Supplemental Data Misuse Information").

- **Temporary Suspension.** If a Participant desires to temporarily suspend the exchange of Data with one or more of the Participants that it believes has permitted or are the subject of the potential or actual Data Misuse pending completion of the Investigation and action of the HSX Board, it shall provide a written Suspension Request Notice ("Suspension Notice") to HSX with a copy to the affected Participant(s) detailing the desired extent of such temporary suspension (i.e., suspend the provision of Data for all Use Cases, certain Data and/or for certain Use Cases) delivered. As soon as possible after receipt of such Suspension Notice, HSX shall convene a telephonic or in person meeting of the HSX Executive Committee to consider the allegations contained in the Data Misuse Notification and the results of HSX's investigation to date. If the HSX Executive Committee believes that the reporting Participant has provided credible information supporting its claims of potential or actual Data Misuse, such potential or actual Data misuse is unresolved and/or, if resolved, was intentional, it shall take such actions as are necessary to temporarily suspend the provision of such notifying Participant's Data to the Participant(s) which are the subject of the potential or actual Data Misuse limiting the suspension, if the technology enables HSX to do so, consistent with the desires of the notifying Participant as contained in the Suspension Notice. Notwithstanding the foregoing, Participant acknowledges that HSX is not able to effectuate the suspension of Data exchanged through Direct Secure Messaging and that it is the obligation of the notifying Participant to instruct its Authorized Users not to send such Data once the suspension is in effect. The HSX Executive Committee may lift any temporary suspension imposed, prior to HSX Board action, with the consent of the notifying Participants(s).

- **HSX Board Action.** Within thirty (30) days of receipt of the written investigative report, the HSX Board shall meet to review the matter and the recommendations contained in the investigative report and shall determine whether to take action including but not limited to termination of a Participant's participation in the HSX Network, lifting or continuing a temporary suspension, requiring additional investigation, or concluding its investigation without taking action against one or more Participants. The HSX Board may require representatives of the affected Participants to be present while it is considering the matter and/or to submit written responses and other information to it for consideration. In making its determinations, the HSX Board shall consider the timeliness and effectiveness of any "cure" by the Participant which is the subject of the potential or actual Data Misuse. The HSX Board shall set forth its actions in writing and provide copies to the affected Participants within five (5) business days after its determination of such action. The actions of the HSX Board shall be implemented in the time frame determined by the HSX Board as described in this Policy notwithstanding a Participant's exercise of the Additional Rights described below.

Additional Rights of Participants. If one or more of the affected Participants does not agree with the action of the Board as described in HSX Board Action section of this Policy, such Participant(s) may avail themselves of the Dispute Resolution Processes in the Participation Agreement, if any, prior to terminating the Participation Agreement for cause (Founding Members may terminate the Participation Agreement for cause pursuant to the provisions of Sections 7.1.2,7.1.3 or 7.1.5) or may terminate the Participation Agreement for convenience. The HSX Board may, but is not obligated to, defer implementation of its actions pending conclusion of such Dispute Resolution Processes.

- **Participants Obligations.** Nothing in this policy shall supersede a Participant's obligations (if any) under relevant Security Incident, Breach Notification or confidentiality provisions of the Participation Agreement or the BAA.

5. Enforcement

- The HSX Chief Privacy Officer, HSX Chief Information Security Officer, President, and the HSX Board of Trustees shall be responsible for enforcing compliance with this Policy.

6. Definitions

For a complete list of definitions, refer to the *Glossary*.

7. References

Policy Owner	Privacy Officer	**Contact**	Don.Reed@healthshareexchange.org
Approved By	HSX Management Team HSX Executive Committee HSX Board	**Approval Date**	November 8, 2018
Date Policy In Effect	January 20, 2016	**Version #**	1.1

1801 Market Street, Suite 750 Philadelphia PA, 19103 www.healthshareexchange.org

Original Issue Date	January 20, 2016	**Last Review Date**	September 15, 2020 November 8, 2018
Related Documents	Acceptable Use Policy Breach Policy Business Associate Agreement Glossary Participation Agreement Sanctions Policy		