COMMONWEALTH HEALTH INSURANCE CONNECTOR AUTHORITY EXCHANGE PRIVACY POLICY AND PROCEDURES

PURPOSE: The Patient Protection and Affordable Care Act and the regulations establishing Exchanges under that act require that an Exchange and its personnel create, collect, use, and disclose Personally Identifiable Information (PII) only when permitted under the Exchange Final Rule, 45 CFR §§ 155.260 and 155.270. This policy is designed to guide Health Connector personnel in implementing these requirements regarding the PII of Health Connector program members.

POLICY: The Health Connector may only create, collect, use, and disclose PII when permitted, as set forth in this policy. The Health Connector will take reasonable steps to limit the creation, collection, use, or disclosure of PII to the minimum necessary to accomplish legitimate business purposes. All Health Connector personnel who need access to PII to carry out their job duties, or who may otherwise come into contact with PII, will be trained on and will be expected to comply with these procedures.

PROCEDURES:

1. Definitions

   Personally Identifiable Information (PII). This policy applies to PII, which is defined as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. includes but is not limited to information collected by the Health Connector for the purpose of determining eligibility for Health Connector programs and health plans, which is governed by 45 CFR §§ 155.260 and 155.270 Additionally PII includes Protected Health Information, Federal Tax Information, Department of Revenue Information and/or M.G.L. Chapter 93H Personal Information. This Policy excludes federal tax information (FTI) which will be safeguarded and disclosed only in accordance with Internal Revenue Service Publication 1075.

2. Required and Permitted Uses and Disclosures of PII

   The Health Connector is permitted to use or disclose PII as follows:

   - To the individual who is the subject of the PII
   - For the purposes of determining eligibility for enrollment in a qualified health plan; determining eligibility for other insurance affordability programs; or determining eligibility for exemptions

- To perform required functions related to oversight and financial integrity
- To evaluate quality improvement strategies and oversee implementation of enrollee satisfaction surveys
- Pursuant to a valid authorization by the individual who is the subject of the PII
- Disclosures required by law to law enforcement individuals

3. Minimum Necessary Requirement

PII will be created, collected, used, or disclosed by or to Health Connector employees or officials, or those under contract with the Health Connector (and, only where necessary, to law enforcement officials), only on a "need to know" basis, meaning only insofar as the PII is necessary to fulfill a legitimate business purpose. The Health Connector may only create, collect, use, or disclose PII to the extent it is necessary to carry out the function(s) listed in Section 2 and never to discriminate inappropriately. Prior to granting employees or officials, or those under contract with the Health Connector access to PII, the Health Connector ensures that these individuals complete appropriate information security and awareness training and then annually thereafter.

Minimum Necessary Use. Health Connector employees who have been given access to databases containing PII may use that access only as necessary to perform assigned work functions. Health Connector employees may be called upon to request PII from other entities, such as MMCOs, in order to perform job functions. When making such requests, Health Connector employees should only request the minimum amount of PII reasonably necessary to perform that function. Health Connector employees may only use or disclose the minimum necessary PII to perform legitimate work functions.

4. Training

Prior to granting employees, contractors and agents access to PII, the Health Connector ensures that these individuals complete appropriate information security and awareness training and then annually thereafter.

5. Security/Safeguards

The Health Connector ensures that its employees, contractors, and agents:

- Implement operational, administrative, physical and technical safeguards to protect PII's confidentiality, integrity, and availability, and to prevent unauthorized or inappropriate access, use, or disclosure of PII
- Understand that they are responsible for safeguarding this information at all times, regardless of whether or not the employee, contractor, or agent is at his or her regular duty station.
- Ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected.
- Send emails containing PII only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information (see IRS Publication 1075 for restrictions on emailing Return Information)
- Limit disclosure of the information and details relating to a PII loss only to those with a need to know

The Health Connector has developed and utilized secure electronic interfaces when sharing personally identifiable information electronically. In addition, the Health Connector has implemented procedures to safeguard the integrity of its information technology assets, including, but not limited to, authentication, monitoring, auditing, and encryption. These security procedures have been integrated into the design, implementation, and day-to-day operations of Health Connector systems as part of our continuing commitment to the security of electronic content as well as the electronic transmission of information. The Health Connector also monitors, periodically assesses, and updates the security controls and related system risks to ensure the continued effectiveness of those controls.

All personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules, as described below.

5. Required and Permitted Uses and Disclosures of PII to the individual subject to the PII

The "Exchange Final Rule," the "Public Records Law," "Fair Information Practices Act," and "HIPAA" provide individuals with certain rights to access their PII contained in the Health Connector's records and the circumstances under the individual can correct this information. The Health Connector follows specific policies and procedures with respect to the individual's access and ability to correct which are detailed in the Health Connector's Policy and Procedures for the Protection of Member Privacy Rights. Questions should be referred to the Privacy Officer.

6. Required and Permitted Uses and Disclosures of PII to Third Parties

To the extent the Health Connector discloses PII to third parties in order to accomplish permitted functions, the Health Connector must enter into written agreements with those third parties that contractually require those third parties to collect, use or disclose PII in accordance with the terms of this policy or more stringent privacy and security standards that meet or exceed applicable regulatory requirements.

7. Required and Permitted Uses and Disclosures of PII Pursuant to Authorizations

PII may be used and disclosed pursuant to a valid authorization by the individual who is the subject of the PII. The authorization is a document signed by the enrollee that gives the Health Connector permission to use specified health information for a specified purpose and time frame. The procedures for obtaining and verifying an authorization are set forth here:

Valid authorization. A valid authorization must be signed and dated by the member. It must identify the person who is authorized to receive the PII. It must state a date at which time the authorization expires. Valid authorization forms that permit the disclosure of PII include an Authorized Representative Designation Form , a Permission to Share Information Form, and a Navigator Designation Form.

Verification. Before PII is disclosed pursuant to an authorization, the Health Connector personnel disclosing the information shall take reasonable steps to verify the identity of the person to whom the disclosure is to be made. Such verification may include examination of official documents, badges, workplace ID cards, driver's license, etc. Any questions should be directed to the Privacy Officer. Further, Health Connector personnel must determine if the expiration date on the authorization has passed; if it has, the authorization is no longer valid.

Revocation of Authorization. The Health Connector will permit any individual to revoke his or his authorization by submitting a request in writing to the Health Connector, as described in the Health Connector's Policy and Procedures for Protection of Member Privacy Rights.

The Health Connector will not make use of disclosures of PII for marketing purposes.

8. Required and Permitted Uses and Disclosures of PII to Law Enforcement

The Health Connector will disclose PII to law enforcement only when necessary and only pursuant to a valid request and/or search warrant.

9. Permitted Disclosures of Aggregate PII

The Health Connector may publicly disclose PII about aggregated Health Connector applicants or members so long as the data meets minimum standards regarding the potential for re-identification (e.g. enrollment by zip code, so long as numbers 10 or less are suppressed or otherwise obscured). Information about individual applicants or members may only be disclosed if it has been de-identified pursuant to the standards found at 45 CFR § 164.514.

10. Unauthorized Disclosures

Although the Health Connector is committed to protecting PII in accordance with this Policy, in the event of an unauthorized disclosure the Health Connector will respond to such disclosure in accordance with its incident/data breach and notification procedures and policies.

11. Destruction of PII

Once a record containing PII is no longer required (and does not otherwise need to be maintained pursuant to the record retention requirements described below), it must be securely destroyed. Secure destruction of PII includes shredding of physical documents or using secure deletion protocols for computer files. If you have questions about destroying electronic PII, please consult the Health Connector's Security Officer.

12. Record Retention

All Health Connector personnel and contractors shall maintain all documents and records (whether paper, electronic, or other media) and other evidence of accounting procedures

and practices related to the following kinds of information for a minimum of ten years from the date of its creation, in compliance with 45 CFR § 155.1210:

a. Information concerning management and operation of the Health Connector's financial and other record keeping systems;
b. Financial statements, including cash flow statements, and accounts receivable and matters pertaining to the costs of operations;
c. Any financial reports filed with other Federal programs or State authorities;
d. Data and records relating to the Health Connector's eligibility verifications and determinations, enrollment transactions, appeals, and plan variation certifications; and
e. Qualified health plan contracting (including benefit review) data and consumer outreach and Navigator grant oversight information.

All Health Connector personnel and contractors shall maintain all documents and records not described above in accordance with the Massachusetts Statewide Records Retention Schedule, found here: http://www.sec.state.ma.us/arc/arcrmu/rmuidx.htm.

APPROVAL:

Louis Gutierrez
Executive Director

Dated: 11/5/15

This policy is subject to annual review.