§ 155.240 Payment of premiums.

(a) Payment by individuals. The Exchange must allow a qualified individual to pay any applicable premium owed by such individual directly to the QHP issuer.

(b) Payment by tribes, tribal organizations, and urban Indian organizations. The Exchange may permit Indian tribes, tribal organizations and urban Indian organizations to pay aggregated QHP premiums on behalf of qualified individuals, including aggregated payment, subject to terms and conditions determined by the Exchange.

(c) Payment facilitation. The Exchange may establish a process to facilitate through electronic means the collection and payment of premiums to QHP issuers.

(d) Required standards. In conducting an electronic transaction with a QHP issuer that involves the payment of premiums or an electronic funds transfer, the Exchange must comply with the privacy and security standards adopted in accordance with § 155.260 and use the standards and operating rules referenced in § 155.270.

§ 155.260 Privacy and security of personally identifiable information.

(a) Creation, collection, use and disclosure. (1) Where the Exchange creates or collects personally identifiable information for the purposes of determining eligibility for enrollment in a qualified health plan; determining eligibility for other insurance affordability programs, as defined in 155.20; or determining eligibility for exemptions from the individual responsibility provisions in section 5000A of the Code, the Exchange may only use or disclose such personally identifiable information to the extent such information is necessary to carry out the functions described in § 155.200 of this subpart unless the creation, collection, use, or disclosure is consistent with this section.

(2) The Exchange may not create, collect, use, or disclose personally identifiable information while the Exchange is fulfilling its responsibilities in accordance with § 155.200 of this subpart unless the creation, collection, use, or disclosure is consistent with this section.

(3) The Exchange must establish and implement privacy and security standards that are consistent with the following principles:

(i) Individual access. Individuals should be provided with a simple and timely means to access and obtain their personally identifiable information in a readable form and format;

(ii) Correction. Individuals should be provided with a timely means to dispute the accuracy or integrity of their personally identifiable information and to have erroneous information corrected or to have a dispute documented if their requests are denied;

(iii) Openness and transparency. There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information;

(iv) Individual choice. Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their personally identifiable information;

(v) Collection, use, and disclosure limitations. Personally identifiable information should be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately;

(vi) Data quality and integrity. Persons and entities should take reasonable steps to ensure that personally identifiable information is complete, accurate, and up-to-date to the extent necessary for the person’s or entity’s intended purposes and has not been altered or destroyed in an unauthorized manner;

(vii) Safeguards. Personally identifiable information should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure; and,

(viii) Accountability. These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods.
should be in place to report and mitigate non-adherence and breaches.

(4) For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure—

(i) The confidentiality, integrity, and availability of personally identifiable information created, collected, used, and/or disclosed by the Exchange;

(ii) Personally identifiable information is only used by or disclosed to those authorized to receive or view it;

(iii) Return information, as such term is defined by section 6103(b)(2) of the Code, is kept confidential under section 6103 of the Code;

(iv) Personally identifiable information is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;

(v) Personally identifiable information is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and

(vi) Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules;

(5) The Exchange must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls.

(6) The Exchange must develop and utilize secure electronic interfaces when sharing personally identifiable information electronically.

(b) Application to non-Exchange entities. Except for tax return information, which is governed by section 6103 of the Code, when collection, use or disclosure is not otherwise required by law, an Exchange must require the same or more stringent privacy and security standards (as §155.260(a)) as a condition of contract or agreement with individuals or entities, such as Navigators, agents, and brokers, that:

(1) Gain access to personally identifiable information submitted to an Exchange; or

(2) Collect, use or disclose personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing the functions outlined in the agreement with the Exchange.

(c) Workforce compliance. The Exchange must ensure its workforce complies with the policies and procedures developed and implemented by the Exchange to comply with this section.

(d) Written policies and procedures. Policies and procedures regarding the creation collection, use, and disclosure of personally identifiable information must, at minimum:

(1) Be in writing, and available to the Secretary of HHS upon request; and

(2) Identify applicable law governing collection, use, and disclosure of personally identifiable information.

(e) Data sharing. Data matching and sharing arrangements that facilitate the sharing of personally identifiable information between the Exchange and agencies administering Medicaid, CHIP or the BHP for the exchange of eligibility information must:

(1) Meet any applicable requirements described in this section;

(2) Meet any applicable requirements described in section 1413(c)(1) and (c)(2) of the Affordable Care Act;

(3) Be equal to or more stringent than the requirements for Medicaid programs under section 1942 of the Act; and

(4) For those matching agreements that meet the definition of "matching program" under 5 U.S.C. 552a(a)(8), comply with 5 U.S.C. 552a(o).

(f) Compliance with the Code. Return information, as defined in section 6103(b)(2) of the Code, must be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code.

(g) Improper use and disclosure of information. Any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the Affordable Care Act will be subject to a civil penalty of not more than $25,000 per person or entity, per use or disclosure, in addition to other penalties that may be prescribed by law.