

(f) *Signature.* For purposes of this section, designation of an authorized representative must be through a written document signed by the applicant or enrollee, or through another legally binding format, as described in § 155.227(a)(2), and must be accepted through all of the modalities described in § 155.405(c).

[78 FR 42313, July 15, 2013]

§ 155.230 General standards for Exchange notices.

(a) *General requirement.* Any notice required to be sent by the Exchange to individuals or employers must be written and include:

(1) An explanation of the action reflected in the notice, including the effective date of the action.

(2) Any factual findings relevant to the action.

(3) Citations to, or identification of, the relevant regulations supporting the action.

(4) Contact information for available customer service resources.

(5) An explanation of appeal rights, if applicable.

(b) *Accessibility and readability requirements.* All applications, forms, and notices, including the single, streamlined application described in § 155.405 and notice of annual redetermination described in § 155.335(c), must conform to the standards outlined in § 155.205(c).

(c) *Re-evaluation of appropriateness and usability.* The Exchange must re-evaluate the appropriateness and usability of applications, forms, and notices.

(d) *Electronic notices.* (1) The individual market Exchange must provide required notices either through standard mail, or if an individual or employer elects, electronically, provided that the requirements for electronic notices in 42 CFR 435.918 are met, except that the individual market Exchange is not required to implement the process specified in 42 CFR 435.918(b)(1) for eligibility determinations for enrollment in a QHP through the Exchange and insurance affordability programs that are effective before January 1, 2015.

(2) The SHOP must provide required notices either through standard mail, or if an employer or employee elects,

electronically, provided that the requirements for electronic notices in 42 CFR 435.918(b)(2) through (5) are met for the employer or employee.

[77 FR 11718, Feb. 27, 2012, as amended at 78 FR 42314, July 15, 2013]

§ 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.

(e) *Premium calculation.* The Exchange may establish one or more standard processes for premium calculation.

(1) For a Federally-facilitated Exchange, the premium for coverage lasting less than one month must equal the product of—

(i) The premium for one month of coverage divided by the number of days in the month; and

(ii) The number of days for which coverage is being provided in the month described in paragraph (e)(1)(i) of this section.

(2) [Reserved]

[77 FR 18444, Mar. 27, 2012, as amended at 79 FR 30346, May 27, 2014]

§ 155.260 Privacy and security of personally identifiable information.

(a) *Creation, collection, use and disclosure.* (1) Where the Exchange creates or

§ 155.260

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 § 155.300; or determining eligibility for exemptions from the individual shared 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:

(i) For the Exchange to carry out the functions described in § 155.200;

(ii) For the Exchange to carry out other functions not described in paragraph (a)(1)(i) of this section, which the Secretary determines to be in compliance with section 1411(g)(2)(A) of the Affordable Care Act and for which an individual provides consent for his or her information to be used or disclosed; or

(iii) For the Exchange to carry out other functions not described in paragraphs (a)(1)(i) and (ii) of this section, for which an individual provides consent for his or her information to be used or disclosed, and which the Secretary determines are in compliance with section 1411(g)(2)(A) of the Affordable Care Act under the following substantive and procedural requirements:

(A) *Substantive requirements.* The Secretary may approve other uses and disclosures of personally identifiable information created or collected as described in paragraph (a)(1) of this section that are not described in paragraphs (a)(1)(i) or (ii) of this section, provided that HHS determines that the information will be used only for the purposes of and to the extent necessary in ensuring the efficient operation of the Exchange consistent with section 1411(g)(2)(A) of the Affordable Care Act, and that the uses and disclosures are also permissible under relevant law and policy.

(B) *Procedural requirements for approval of a use or disclosure of personally identifiable information.* To seek approval for a use or disclosure of personally identifiable information created or collected as described in paragraph (a)(1) of this section that is not described in paragraphs (a)(1)(i) or (ii) of

45 CFR Subtitle A (10–1–16 Edition)

this section, the Exchange must submit the following information to HHS:

(1) Identity of the Exchange and appropriate contact persons;

(2) Detailed description of the proposed use or disclosure, which must include, but not necessarily be limited to, a listing or description of the specific information to be used or disclosed and an identification of the persons or entities that may access or receive the information;

(3) Description of how the use or disclosure will ensure the efficient operation of the Exchange consistent with section 1411(g)(2)(A) of the Affordable Care Act; and

(4) Description of how the information to be used or disclosed will be protected in compliance with privacy and security standards that meet the requirements of this section or other relevant law, as applicable.

(2) The Exchange may not create, collect, use, or disclose personally identifiable information 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—(1) Non-Exchange entities.* A non-Exchange entity is any individual or entity that:

(i) Gains access to personally identifiable information submitted to an Exchange; or

(ii) Collects, uses, or discloses personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or entity is performing functions agreed to with the Exchange.

(2) Prior to any person or entity becoming a non-Exchange entity, Exchanges must execute with the person or entity a contract or agreement that includes:

(i) A description of the functions to be performed by the non-Exchange entity;

(ii) A provision(s) binding the non-Exchange entity to comply with the privacy and security standards and obligations adopted in accordance with paragraph (b)(3) of this section, and specifically listing or incorporating those privacy and security standards and obligations;

(iii) A provision requiring the non-Exchange entity to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with paragraph (a)(5) of this section;

(iv) A provision requiring the non-Exchange entity to inform the Exchange of any change in its administrative, technical, or operational environments defined as material within the contract; and

(v) A provision that requires the non-Exchange entity to bind any downstream entities to the same privacy and security standards and obligations to which the non-Exchange entity has

§ 155.270

agreed in its contract or agreement with the Exchange.

(3) When collection, use or disclosure is not otherwise required by law, the privacy and security standards to which an Exchange binds non-Exchange entities must:

(i) Be consistent with the principles and requirements listed in paragraphs (a)(1) through (6) of this section, including being at least as protective as the standards the Exchange has established and implemented for itself in compliance with paragraph (a)(3) of this section;

(ii) Comply with the requirements of paragraphs (c), (d), (f), and (g) of this section; and

(iii) Take into specific consideration:

(A) The environment in which the non-Exchange entity is operating;

(B) Whether the standards are relevant and applicable to the non-Exchange entity's duties and activities in connection with the Exchange; and

(C) Any existing legal requirements to which the non-Exchange entity is bound in relation to its administrative, technical, and operational controls and practices, including but not limited to, its existing data handling and information technology processes and protocols.

(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;

45 CFR Subtitle A (10–1–16 Edition)

(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 CMP of not more than \$25,000 as adjusted annually under 45 CFR part 102 per person or entity, per use or disclosure, consistent with the bases and process for imposing civil penalties specified at §155.285, in addition to other penalties that may be prescribed by law.

[77 FR 18444, Mar. 27, 2012, as amended at 77 FR 31515, May 29, 2012; 79 FR 13837, Mar. 11, 2014; 79 FR 30346, May 27, 2014; 81 FR 12341, Mar. 8, 2016; 81 FR 61581, Sept. 6, 2016]

§ 155.270 Use of standards and protocols for electronic transactions.

(a) *HIPAA administrative simplification.* To the extent that the Exchange performs electronic transactions with a covered entity, the Exchange must use standards, implementation specifications, operating rules, and code sets that are adopted by the Secretary in 45 CFR parts 160 and 162 or that are otherwise approved by HHS.

(b) *HIT enrollment standards and protocols.* The Exchange must incorporate interoperable and secure standards and protocols developed by the Secretary in accordance with section 3021 of the PHS Act. Such standards and protocols must be incorporated within Exchange information technology systems.

[77 FR 18444, Mar. 27, 2012, as amended at 78 FR 54135, Aug. 30, 2013]