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 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;

(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]

§ 155.280 Oversight and monitoring of privacy and security requirements.

(a) *General.* HHS will oversee and monitor the Federally-facilitated Exchanges, State-based Exchanges on the Federal platform, and non-Exchange entities required to comply with the privacy and security standards established and implemented by a Federally-facilitated Exchange pursuant to § 155.260 for compliance with those standards. HHS will oversee and monitor State Exchanges for compliance with the standards State Exchanges establish and implement pursuant to § 155.260. State Exchanges will oversee and monitor non-Exchange entities required to comply with the privacy and security standards established and implemented by a State Exchange in accordance to § 155.260.

(b) *Audits and investigations.* HHS may conduct oversight activities that include but are not limited to the following: audits, investigations, inspections, and any reasonable activities necessary for appropriate oversight of compliance with the Exchange privacy and security standards. HHS may also pursue civil, criminal or administrative proceedings or actions as determined necessary.

[78 FR 54135, Aug. 30, 2013, as amended at 81 FR 12341, Mar. 8, 2016]

§ 155.285 Bases and process for imposing civil penalties for provision of false or fraudulent information to an Exchange or improper use or disclosure of information.

(a) *Grounds for imposing civil money penalties.* (1) HHS may impose civil money penalties on any person, as defined in paragraph (a)(2) of this section, if, based on credible evidence, HHS reasonably determines that a person has engaged in one or more of the following actions:

(i) Failure to provide correct information under section 1411(b) of the Affordable Care Act where such failure is attributable to negligence or disregard of any rules or regulations of the Secretary with negligence and disregard defined as they are in section 6662 of the Internal Revenue Code of 1986:

(A) ‘‘Negligence’’ includes any failure to make a reasonable attempt to provide accurate, complete, and comprehensive information; and

(B) ‘‘Disregard’’ includes any careless, reckless, or intentional disregard for any rules or regulations of the Secretary.

(ii) Knowing and willful provision of false or fraudulent information required under section 1411(b) of the Affordable Care Act, where knowing and willful means the intentional provision of information that the person knows to be false or fraudulent; or

(iii) Knowing and willful use or disclosure of information in violation of section 1411(g) of the Affordable Care Act, where knowing and willful means the intentional use or disclosure of information in violation of section 1411(g). Such violations would include, but not be limited to, the following:

(A) Any use or disclosure performed which violates relevant privacy and security standards established by the Exchange pursuant to § 155.260;

(B) Any other use or disclosure which has not been determined by the Secretary to be in compliance with section 1411(g)(2)(A) of the Affordable Care Act pursuant to § 155.260(a); and

(C) Any other use or disclosure which is not necessary to carry out a function described in a contract with a non-Exchange entity executed pursuant to § 155.260(b)(2).

(2) For purposes of this section, the term ‘‘person’’ is defined to include, but is not limited to, all individuals; corporations; Exchanges; Medicaid and CHIP agencies; other entities gaining access to personally identifiable information submitted to an Exchange to carry out additional functions which