135.156E Legal and policy.

1. Upon approval from the board, the department shall implement appropriate security standards, policies, and procedures to protect the transmission and receipt of protected health information exchanged through the Iowa health information network, which shall, at a minimum, comply with the Health Insurance Portability and Accountability Act security rule pursuant to 45 C.F.R. pt. 164, subpt. C, and shall reflect all of the following:

a. Include authorization controls, including the responsibility to authorize, maintain, and terminate a participant's use of the Iowa health information network.

b. Require authentication controls to verify the identity and role of the participant using the Iowa health information network.

c. Include role-based access controls to restrict functionality and information available through the Iowa health information network.

d. Include a secure and traceable electronic audit system to document and monitor the sender and the recipient of health information exchanged through the Iowa health information network.

e. Require standard participation agreements which define the minimum privacy and security obligations of all participants using the Iowa health information network and services available through the Iowa health information network.

f. Include controls over access to and the collection, organization, and maintenance of records and data for purposes of research or population health that protect the confidentiality of consumers who are the subject of the health information.

2. A patient shall have the opportunity to decline exchange of the patient's health information through the Iowa health information network. A patient shall not be denied care or treatment for declining to exchange the patient's health information, in whole or in part, through the Iowa health information network. The board shall provide by rule the means and process by which patients may decline participation. The means and process utilized under the rules shall minimize the burden on patients and health care professionals.

3. Unless otherwise authorized by law or rule, a patient's decision to decline participation means that none of the patient's health information shall be accessible through the record locator service function of the Iowa health information network. A patient's decision to decline having health information shared through the record locator service function shall not limit a health care professional with whom the patient has or is considering a treatment relationship from sharing health information concerning the patient through the secure messaging function of the Iowa health information network.

4. A patient who declines participation in the Iowa health information network may later decide to have health information shared through the Iowa health information network. A patient who is participating in the Iowa health information network may later decline participation in the network.

5. A participant shall not release or use protected health information exchanged through the Iowa health information network for purposes unrelated to prevention, treatment, payment, or health care operations unless otherwise authorized or required by state or federal law. Participants shall limit the use and disclosure of protected health information for payment or health care operations to the minimum amount required to accomplish the intended purpose of the use or request, in compliance with the Health Insurance Portability and Accountability Act and other applicable state or federal law. Use or distribution of the information for a marketing purpose, as defined by the Health Insurance Portability and Accountability Act, is strictly prohibited.

6. The department and all persons using the Iowa health information network are individually responsible for following breach notification policies as provided by the Health Insurance Portability and Accountability Act.

7. A participant shall not be compelled by subpoena, court order, or other process of law to access health information through the Iowa health information network in order to gather records or information not created by the participant.

8. All participants exchanging health information and data through the Iowa health information network shall grant to other participants of the network a nonexclusive license

to retrieve and use that information in accordance with applicable state and federal laws, and the policies, standards, and rules established by the board.

9. The board shall establish by rule the procedures for a patient who is the subject of health information to do all of the following:

a. Receive notice of a violation of the confidentiality provisions required under this division.

b. Upon request to the department, view an audit report created under this division for the purpose of monitoring access to the patient's health care information.

10. A health care professional who relies reasonably and in good faith upon any health information provided through the Iowa health information network in treatment of a patient who is the subject of the health information shall be immune from criminal or civil liability arising from any damages caused by such reasonable, good-faith reliance. Such immunity shall not apply to acts or omissions constituting negligence, recklessness, or intentional misconduct.

11. A participant that has disclosed health information through the Iowa health information network in compliance with applicable law and the standards, requirements, policies, procedures, and agreements of the network shall not be subject to criminal or civil liability for the use or disclosure of the health information by another participant.

12. Notwithstanding chapter 22, the following records shall be kept confidential, unless otherwise ordered by a court or consented to by the patient or by a person duly authorized to release such information:

a. The protected health information contained in, stored in, submitted to, transferred or exchanged by, or released from the Iowa health information network.

b. Any protected health information in the possession of the department due to its administration of the Iowa health information network.

13. Unless otherwise provided in this division, when using the Iowa health information network or a private health information network maintained in this state that complies with the privacy and security requirements of this chapter for the purposes of patient treatment, a health care professional or a hospital is exempt from any other state law that is more restrictive than the Health Insurance Portability and Accountability Act that would otherwise prevent or hinder the exchange of patient information by the patient's health care professional or hospital.

2012 Acts, ch 1080, §14, 17; 2012 Acts, ch 1138, §48, 80, 81
[T] NEW section