Overview

This bill allows a health care provider to designate credentials verification entities to collect, verify, maintain, and store core credentials data on the provider and to provide the data collected to health care entities, the commissioner of health, and health-related licensing boards that are authorized to obtain the data. A health care provider can designate a single entity to maintain the provider's credentials data, submit updated information to that entity as necessary, and refer a health care entity, the commissioner, or a licensing board to the designated verification entity for information on the provider's credentials.

1 Definitions. Adds § 145D.01. Defines the following terms, for a chapter governing credentials verification entities for health care providers: certified, core credential data, credentialing, credentials verification entity, commissioner, designated credentials verification entity, health care entity, health care provider, health-related licensing board, national accrediting organization, primary source verification, recredentialing, and secondary source verification.

2 Designated credentials verification entity. Adds § 145D.02. Allows a health care provider to designate a credentials verification entity to collect, verify, maintain, and store provider core credentials data and provide that data to an authorized requesting entity. Requires a provider who designates a credentials verification entity to report core credentials data to the entity and to update the data as needed and quarterly. Requires health care entities to use designated credentials verification entities to obtain core credentials data, if the provider has made such a designation.

Subd. 1. Designation. Allows a health care provider to designate a credentials verification entity to collect, verify, maintain, and store the health care provider's core credentials data, and provide that data to a health care entity, health-related licensing board, or the commissioner of health. Provides that once the core credentials data are submitted to a credentials verification entity, the health care provider is not required to resubmit this data to a health care entity when applying for practice privileges or participating provider status. Requires a health care provider to submit updated information as needed to ensure that the credentialing data are current.
Subd. 2. Reporting core credentials data. Requires a health care provider to report core credentials data and any modifications to existing data to the provider's designated credentials verification entity as soon as possible, but not later than 30 days after a change occurs or the new information is known. Also requires a provider to update the provider's data at least quarterly, on a form provided by the credentials verification entity.

Subd. 3. Use of the designated credentials verification entity. Requires a health care entity to use a credentials verification entity designated by a health care provider to obtain core credentials data on a provider applying for privileges or participating provider status with that entity, if the provider has designated a credentials verification entity. Allows the health care entity, its contractee, or the designated credentials verification entity to collect any additional information required for the health care entity's credentialing process, from the primary source of that information.

Subd. 4. Additional credentialing information. States that this chapter does not restrict the right of any health care entity to request additional information for credentialing.

Subd. 5. Access to national practitioner data bank. States that this chapter does not restrict access to the National Practitioner Data Bank by the commissioner, a health-related licensing board, a health care entity, or a credentials verification entity.

3 Duplication of data prohibited. Adds § 145D.03. Prohibits health care entities and credentials verification entities from collecting or trying to collect duplicate core credentials data from a health care provider or any primary source of information if the provider has a designated credentials verification entity and if the information is already on file with the designated credentials verification entity.

Subd. 1. Prohibition on a health care entity. Prohibits a health care entity from collecting or trying to collect duplicate core credentials data from a health care provider or any primary source if the health care provider has a designated credentials verification entity and the provider has notified the health care entity of the designation.

Subd. 2. Prohibition on a credentials verification entity. Prohibits a credentials verification entity from trying to collect duplicate core credentials data from a health care provider or from any primary source if the information is already on file with another credentials verification entity designated by the provider, unless otherwise authorized by the provider.

4 Availability of data collected. Adds § 145D.04. Requires a credentials verification entity to make available to a health care entity, the commissioner, or a health-related licensing board, upon request, all core credentials data it collects on any health care provider. Allows a credentials verification entity to charge a reasonable fee to access the data, not to exceed the actual cost of a health care entity collecting and verifying the data.

5 Standards. Adds § 145D.05. Requires any credentials verification entity doing business in Minnesota to meet national standards that are approved by a national accrediting organization.

6 Recredentialing. Adds § 145D.06. Prohibits a health care entity from requiring a health care provider who already has privileges with that entity to be re-credentialied just because the provider has changed practice location or affiliation.

7 Reimbursement. Adds § 145D.07. Requires a health care entity to continue to reimburse a health care provider whose core credentials have been verified, while the provider is in the process of being re-credentialled.

8 Liability. Adds § 145D.08. Prohibits civil, criminal, and administrative actions from being instituted against, and extends immunity from liability to, a health care entity that relies on data obtained from a credentials verification entity that meets the requirements of this chapter.