The MARYLAND HEALTH CARE COMMISSION

COMAR 10.25.19 State Recognition of an Electronic Advance Directives Service

Draft Criteria for State Recognition of an Electronic Advance Directives Service

For Public Comment

Proposed regulations regarding State Recognition of an Electronic Advance Directives Service, adopted by the Maryland Health Care Commission (MHCC or Commission) as final regulations on February 15, 2018 will require, at COMAR 10.25.19.03B, that the Commission publish in the Maryland Register and on its website draft criteria to be considered by the Commission in reviewing an application by an Electronic Advance Directives Service for State Recognition, a prerequisite for connecting to the State-Designated Health Information Exchange. The draft criteria were developed by Commission staff after meetings with stakeholders in the fall of 2016. In general, the draft criteria include standards for privacy and security, auditing and compliance, and education, reporting, and technical provisions, some of which are required by State and/or federal law.

The MHCC seeks public comments on this draft criteria. Comments will be accepted until 4:30 p.m. on Friday, March 30, 2018 and should be submitted via email to Christine Karayinopulous at **christine.karayinopulos@maryland.gov** or via mail to:

Maryland Health Care Commission
ATTN: Christine Karayinopulous
4160 Patterson Ave
Baltimore, MD 21215

Comments are due by 4:30 p.m. on Friday, March 30, 2018

Maryland Health Care Commission

Draft Criteria for State Recognition of an Electronic Advance Directives Service

A. Policies and Procedures – Each electronic advance directives service vendor ("Vendor") shall submit copies of its policies and procedures regarding the following areas.

1. Method for assigning each declarant or health care agent (hereafter referred to as "consumer") a unique user name and password.

2. Procedural and technical controls (e.g., authorization and authentication) for the exchange of health information with a third party, including exchange through a health information exchange (HIE).

3. Appropriate administrative, physical, and technical safeguards that, at a minimum, meet the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and meet State-specific requirements, including notice of privacy practices to consumers.

4. Assessment of a potential breach and responding to a breach, including investigation processes, remedial action plans, notifications to consumers and MHCC (and others as required by State or federal law), and suspension or termination of access and notifications.1

5. Methods for uploading a paper-based advance directive and for creating an electronic advance directive, including: version control protocols for multiple advance directives; sharing and deletion of advance directives; and identification of the types of individuals/entities that can obtain access to information in the Vendor's advance directives database/repository

6. Transfer of electronic advance directives if the Vendor is sold or goes out of business; and provision of notification to consumers, within a reasonable cure period so that consumers may make alternative arrangements for securing their data (Note: Vendor must agree to escrow any data for Maryland residents for a specified time period upon request by MHCC).

7. Communication with end-users of the technology (e.g., consumers, health care providers, etc.), including methods, frequency, and anticipated reason for communications.

8. Identification of circumstances, if any, under which mailing lists/contact information can be shared or sold.

9. Disaster recovery, business continuity, and cybersecurity.

B. Auditing and Compliance – Each Vendor shall provide supporting documentation of its compliance with the following criteria.

1. At least annually, the results from an independent third party privacy and security audit that reviews and tests security controls, including appropriate and permitted access, use, and disclosure of protected health information (PHI) – to include subcontractors, such as data centers.

2. Certification or accreditation by a nationally recognized third party privacy and security organization (e.g., EHNAC, SOC II).

C. Technical – Each Vendor shall provide evidence that it meets or exceeds the following criteria. Note: items with an asterisk (*) required by law.

1. Offers a secure, web-based application to create, update, and store electronic advance directives consistent with the Health Level-7, Consolidated Clinical Document Architecture Personal Advance Care Plan document standard.

2. Allows a consumer to download their advance directive into a printable document or electronically transfer it to another system or third party.

3. Uses, at a minimum, remote identity proofing in accordance with Authenticator Assurance Level 2 of the National Institute of Standards and Technology *(NIST Special Publications 800-63-3 (Digital Identity Guidelines) and 800-63A (Digital Identity Guidelines: Enrollment and Identity Proofing).**

4. Accepts video recordings for electronic advance directives, allowing a declarant to express health care wishes and appoint a personal health care agent.*

5. Stores paper-based advance directives received by fax or other electronic means* and makes the paper-based advance directives as easily retrievable as electronic advance directives created via the vendor's website.

6. Collects consumer demographics consistent with key data elements required by the State-Designated HIE Master Patient Index to assist in appropriately matching patients.

7. Allows a consumer to delete their electronic advance directive.

8. Tracks information on when and by whom an advance directive was created, updated, accessed, or deleted.

9. Makes available only completed and signed electronic advance directives to appropriately authorized individuals (e.g., health care agent or proxy, health care providers, etc.) and the State-Designated HIE.

10. Uses at least 12 point font consistent with U.S. Department of Health & Human Services Usability Guidelines.

D. Reporting – Each Vendor shall attest that it can and will provide the following reports.

1. At least biannually, report the number of unique advance directives on file for Maryland residents and the number of times a unique advance directive has been queried (i.e., opened/viewed) through the State-Designated HIE by provider type.

2. Report each instance of a breach involving Maryland residents and steps for remediation as provided in COMAR 10.25.18.08.

3. Produce ad hoc reports at the request of the State.

E. Education – Each Vendor shall provide documentation of its compliance with the following criteria.

1. Has educational materials for consumers that details the Vendor's scope of services, warranties, and any costs associated with electronic advance directive services. The educational materials shall, at a minimum:

   a. Disclose any cost to a consumer prior to the consumer's creation of an electronic advance directive or upload of a paper-based advance directive;

   b. Advise consumers regarding provision of advance notice of any change in fees;

   c. Give notice of integration with the State-Designated HIE and any other third party, and include a disclosure that only complete advance directives will be accessible to authorized individuals via the State-Designated HIE; and

   d. Notice identifying those who can access advance directives through the State-Designated HIE.

F. Connectivity with the State-Designated HIE – Each Vendor shall provide documentation of its compliance with the following technical requirements.

1. Establishment of application programming interfaces (APIs) that are consistent with current specifications from the State-Designated HIE that will permit a third party to determine if an advance directive exists and to retrieve structured and non-structured information contained in the advance directive.

2. Development of APIs that permit a third party to create an advance directive form from a third party system.

3. Adherence to current protocols including Advanced Encryption Standards (AES) and Transport Layer Security (TLS) for the protection of data at rest and in transit.