



Criteria for State Recognition of an Electronic Advance Directives Service

For Public Comment

Released Friday, July XX, 2022

State law (2016 Chapter 510 and 2017 Chapter 667) required the Maryland Health Care Commission (MHCC) to develop a State Recognition Program for electronic advance directives services (vendors). The law aims to facilitate use of cloud-based technology to support creation of and accessibility to electronic advance directives. State Recognition demonstrates a vendor meets certain criteria or standards for privacy and security, independent audits, education, reporting, and technical provisions, some of which are required by State and federal law. During the 2022 session of the Maryland General Assembly, Chapter 312 (Senate Bill 824), *Health – Accessibility of Electronic Advance Care Planning Documents*, repealed the requirement that vendors implement a certain electronic authorization guideline (NIST¹ Special Publication 800–63–2: Electronic Authentication Guideline or subsequent replacement publications to 800-63) to connect to the State Designated Health Information Exchange.

The MHCC seeks public comment on the draft vendor criteria for State Recognition (Version 2.0 – July 2022).² The criteria exclude the NIST requirement to align with the law and include other miscellaneous changes; **material changes are highlighted in yellow**. Public comments will be accepted until 4:30pm on **August XX, 2022**; comments should be submitted via email or by mail to:

Justine Springer at justine.springer@maryland.gov; or
Maryland Health Care Commission
ATTN: Justine Springer
4160 Patterson Ave
Baltimore, MD 21215

¹ NIST is the acronym for the National Institute of Standards and Technology, a non-regulatory government agency.

² Current vendor criteria for State Recognition (Version 1.0 – April 2018) is available here:

mhcc.maryland.gov/mhcc/pages/hit/hit_advancedirectives/documents/AD_Criteria_20180423.pdf.

CRITERIA FOR STATE RECOGNITION

State Recognition of an electronic advance directives service (or “Vendor”) is a component of a statewide Advance Directives Program required by law³ that aims to facilitate use of cloud-based technology to support creation of and accessibility to electronic advance directives. State Recognition is a prerequisite for a Vendor to connect to the State-Designated Health Information Exchange (HIE).

A. POLICIES AND PROCEDURES

Each Vendor shall demonstrate policies for the following:

1. Method for assigning each declarant or health care agent (or “consumer”) a unique username and password.
2. Procedural and technical controls (e.g., authorization and authentication) for the exchange of health information with an 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.
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

³ 2016 Chapter 510; 2017 Chapter 667; and 2022 Chapter 312.

DRAFT

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. INDEPENDENT AUDITS

Each Vendor and subcontractor(s) that maintains and supports the technical infrastructure on behalf of the Vendor shall **annually** demonstrate evidence of adequate systems and privacy and security controls by providing appropriate documentation from an independent third-party.

1. Evidence may include the most recent documentation summarizing the status of compliance with recognized security practices, including a Service Organization Control (SOC) 2 Type 2 attestation, **or accreditation or certification by a nationally recognized entity**.

C. TECHNICAL

Each Vendor shall demonstrate it meets or exceeds the following criteria:

Note: Items with an asterisk () are 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 consumers to download advance directives into a printable document or electronically transfer to another system or third party.
3. Accepts video recordings for electronic advance directives, allowing a declarant to express health care wishes and appoint a personal health care agent.*⁴

⁴ See Maryland Code Annotated, Health-General Article § 5-602(c)(3) (Supp. 2022).

DRAFT

4. Stores paper-based advance directives received by facsimile or other electronic means⁵ and makes the paper-based advance directives as easily retrievable as electronic advance directives created via the vendor's website.
5. Collects consumer demographics consistent with key data elements required by the State-Designated HIE Master Patient Index to assist in appropriately matching patients.
6. Allows consumers to delete their electronic advance directives.
7. Tracks information on when and by whom an advance directive was created, updated, accessed, or deleted.
8. 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.
9. 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 **quarterly**, report the number of unique advance directives for Maryland residents in a manner specified by MHCC.
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 Commission.

E. EDUCATION CONTENT

Each Vendor shall provide documentation of consumer notifications and educational materials for the following that minimally discloses costs, scope of services, warranties, and privacy of security practices:

1. Fees associated with the electronic advance directives service.

⁵ See Maryland Code Annotated, Health-General Article § 19-144(b)(3) (Supp. 2017).

DRAFT

2. Amount(s) and effective date(s) for any change(s) in fees.
3. Integration with the State-Designated HIE and any other third party, noting that only complete advance directives will be accessible to authorized users.
4. Actions that can be taken if State Recognition is not renewed, suspended, or revoked.
5. Information on how personal information is protected, how the information may be used and with whom it may be shared with, when and how notice is provided if personal information is compromised, and steps to take in the event of a breach.

F. CONNECTIVITY WITH THE STATE-DESIGNATED HIE

Each Vendor shall demonstrate its ability to comply with the following technical requirements:

1. Establishment and maintenance 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 or non-structured information contained in the advance directive.
2. Adherence to current protocols including AES (Advanced Encryption Standards) and TLS (Transport Layer Security) for the protection of data at rest and in transit.