MARYLAND HEALTH CARE COMMISSION

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 law[1] 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). If an applicant is unable to meet certain criteria, a written explanation must be submitted with its application detailing the circumstances.

A. Policies and Procedures – Each electronic advance directives service shall submit copies of its policies regarding the following areas.

1. Method for assigning each declarant or health care agent (or "consumer") a unique user name 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.[2]
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.[2]
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.

[1] 2016 Chapter 510 and 2017 Chapter 667.
[2] NOTE: Copies of policies and procedures for Criteria A.3 and A.4 need not be provided if the Vendor demonstrates compliance with HIPAA and HITECH in Criteria B. Independent Audits.

B. Independent Audits – Each Vendor shall provide supporting documentation of its compliance with the following criteria.

1. Evidence that a Service Organization Control (SOC) 2 Type 2 audit is conducted annually for the Vendor and any subcontractor(s) that maintain and support the technical infrastructure on behalf of a Vendor.
2. Copy of the most recent SOC report(s) and remediation plans to address the exceptions identified.

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. Uses, at a minimum, (Identity Assurance Level) IAL2 of the National Institute of Standards and Technology Special Publications 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*.*[3]
4. Accepts video recordings for electronic advance directives, allowing a declarant to express health care wishes and appoint a personal health care agent.*[4]
5. Stores paper-based advance directives received by facsimile or other electronic means*[5] 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 consumers to delete their electronic advance directives.
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.

---

[3] *See* Maryland Code Annotated, Health-General Article § 5-602 (c)(3) (Supp. 2017) (citing NIST Special Publication (SP) 800-63-2). Subsequent to the enactment of Health-General Article § 5-602 (c)(3) in 2016, information security standards and guidelines have changed as updated in NIST SP 800-63-3, published June 2017, which supersedes NIST SP 800-63-2.

[4] *See* Maryland Code Annotated, Health-General Article § 5-602(c)(4) (Supp. 2017).

[5] *See* Maryland Code Annotated, Health-General Article § 19-144(b)(4) (Supp. 2017).

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 Commission.

E. Education Content – 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:
    i. 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;
    ii. Advise consumers regarding provision of advance notice of any change in fees;
    iii. 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 users via the State-Designated HIE; and
    iv. Notice identifying those who can access advance directives through the State-Designated HIE.

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.