State Recognition of an Electronic Advance Directives Service

Renewal Application – ADVault, Inc.

July 15, 2021

Draft

MARYLAND HEALTH CARE COMMISSION

Center for Health Information Technology
and Innovative Care Delivery

Background

- State law aims to facilitate use of cloud-based technology that supports creation of and accessibility to electronic advance directives, and required MHCC to develop a State Recognition Program for electronic advance directives services (or vendors)
- COMAR 10.25.19, *State Recognition of an Electronic Advance Directives Service* (effective March 12, 2018), outlines program procedures for State Recognition
  - Vendors awarded State Recognition by MHCC may connect to the State-Designated Health Information Exchange (HIE)
  - State Recognition is valid for three years unless suspended or revoked by MHCC
- One vendor has sought and obtained State Recognition since 2018

(See appendix for background information on the law)

Vendor Profile

- ADVault, Inc. is a Texas corporation that began operations in 2007
- The electronic advance directive service is a free, web-based application for consumers to create, update, store, and share electronic advance directives
  (see appendix for information on volume of advance directives stored in the repository)
- Competitively selected by MHCC in 2013 to integrate its web-based repository with CRISP; interface launched 2014 allowing authorized health care providers to access electronic advance directives via CRISP created on MyDirectives.com
- Initial State Recognition received in July 2018

Privacy and Security Safeguards

- Audit tools track when electronic advance directives are created, updated, accessed, and deleted (including time and date stamps, geographic locators, IP addresses, etc.)
- An independent auditor annually reviews vendor's policies and procedures for protecting electronic health information, disaster recovery, business continuity, cybersecurity, and breach assessment and response
- ADVault achieved HITRUST CSF Certification in June 2020, certification based on meeting national standards on security control structure *(see appendix for information about HITRUST)*
- Application software and data storage provided by third-party vendors undergo annual SOC 2 audits that report on controls relevant to security, processing integrity, and confidentiality principles of the system *(see appendix for information about SOC 2)*

Consumer Features and Authentication

- Web-based application allows consumers to name a health care agent, create a digital advance care plan, or upload an existing (paper-based) document
- Electronic advance directives can be downloaded, printed, transferred to another system, or deleted
- Supports video advance directives
- Uses remote identity proofing in accordance with NIST to establish that Maryland residents are who they claim to be *(see appendix for information about NIST)*

Commission Action

Staff recommends the Commission renew State Recognition for ADVault, Inc.

Appendix

Electronic Advance Directive Volume

- The ADVault repository has roughly 4,882 electronic advance directives (as of Q1 2021) consisting of:
  - 2,486 Advance Care Plans
  - 2,074 Health Care Agents
  - 322 Document Uploads
- All hospital electronic health record systems offer a minimum set of features required by ONC certification -- includes functionality to store advance directives
- A scan of 9 hospitals in 2020 found that new advance directives added annually to their EHR systems (Cerner, Epic, and Meditech) since 2018 total over 25,000
  - 7,068 in 2018; 8,893 in 2019; and 9,373 through Q3 2020

Legislation Background

- House Bill 1106, *Public Health – Electronic Advance Directives – Witness Requirements* (2015)
  - Requires two witnesses for electronic signature on an advance directive outside the presence of the declarant who signed the advance directive if it was created in compliance with electronic witness protocols of MDH
- House Bill 1385, *Public Health – Advance Directives – Procedures, Information Sheet, and Use of Electronic Advance Directives* (2016)
  - Alters witness requirements for an electronic advance directive and expands the scope of education and outreach efforts, including required content of an advance directive information sheet and the distribution process; requires MHCC to develop a State Recognition Program

Legislation Background *(Cont.)*

- House Bill 0188, *Public Health – Advance Directives – Witness Requirements, Advance Directives Services, and Fund* (2017)
  - Clarifies the definition of an advance directive; clarifies that MDH may contract with one or more vendors; establishes a non-lapsing Advance Directives Program Fund

The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)

- A comprehensive and certifiable framework used by organizations that create, access, store, or exchange sensitive data.
- Consist of a prescriptive set of controls comprised of industry guidelines, standards, and best practices developed by experts across various disciplines, industries, government, and academia
- Harmonizes the requirements of multiple regulations and standards (HIPAA, ISO, NIST, etc.)
- Serves as a roadmap to help organizations maintain compliance and continually improve cybersecurity

System and Organizational Controls (SOC) 2

- Comprehensive reporting framework put forth by the American Institute of Certified Public Accountants
- Independent third-party auditors (licensed CPA firms) assess and subsequently test controls relating to Trust Services Criteria (previously Trust Services Principles) implemented across an organization and its IT infrastructure
- SOC 2 reports provide assurance about the controls at a service organization, including oversight, vendor management programs, corporate governance and risk management processes, and regulatory compliance oversight

National Institute of Standards and Technology (NIST)

- NIST offers guidelines on technology-related matters to protect and keep data safe
  - Standards provide a level of uniformity when it comes to cybersecurity
- Identity Assurance Levels (IALs) are a key component of the NIST Digital Identity Guidelines, NIST 800-63-3
  - Standards verify that people are who they say they are
  - IAL2 requires identity proofing, which can be completed remotely or in person