Security Whitepaper

Introduction

DeVero, Inc. is a cloud-based, software-as-a-service (SaaS) company that provides a HIPAA-compliant, highly-scalable and unique intelligent data capture, management and integration solution for healthcare companies. This 100% online service makes it easy for home healthcare agencies, hospice agencies, private duty companies, therapy groups, and other healthcare businesses to go paperless. Companies use DeVero to transition from paper to electronic documentation in order to overcome their paper overload, streamline their operations, improve cash flow, and provide visibility and management of their operations from any place at any time using any device with an industry-standard web browser.

DeVero's highly-secure offering is used by a wide range of healthcare companies including startup agencies to the largest public home health chain in the United States. Currently, DeVero has over 75,000 active users including nurses, therapists, health aides, physicians, office workers, and other disciplines and user types.

DeVero is compliant with HIPAA's privacy and security rules including the requirement to:

- Ensure the confidentiality, integrity and availability of all electronic protected health information (EPHI) received, maintained and/or transmitted
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by DeVero's workforce

Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information".

The HIPAA Security Rule specifically focuses on the safeguarding of EPHI including protecting the confidentiality, integrity, and availability of EPHI.

DeVero's compliance with the security rule includes implementation of the following safeguards:

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards

The individual safeguards are described below.

Administrative Safeguards

DeVero implements the necessary administrative actions, policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of DeVero's workforce in relation to the protection of that information.

DeVero addresses the following administrative safeguards:

Security Management Process

DeVero implements policies and procedures to prevent, detect, contain and correct security violations. These policies and procedures are as follows:

Risk Analysis
DeVero conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI provided to DeVero by covered entity.

Risk Management
DeVero implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Sanction Policy
DeVero applies appropriate sanctions against its workforce members who fail to comply with the security policies and procedures of DeVero.

Information System Activity Review
DeVero implements procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports as needed.

Assigned Security Responsibility

DeVero has designated a HIPAA Security Officer who is responsible for the development and implementation of the policies and procedures required by the security rule.

Workforce Security

DeVero has implemented policies and procedures to ensure that all members of its workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining access to EPHI. The following policies and procedures address workforce security:

Authorization and Supervision
DeVero has implemented policies and procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.

Workforce Clearance Procedure
DeVero has implemented procedures to determine that the access of a workforce member to EPHI is appropriate.

Termination Procedures
DeVero has implemented procedures for terminating access to EPHI when the employment of, or other arrangement with, a workforce member ends.

Information Access Management

DeVero has implemented policies and procedures for authorizing access to EPHI that are consistent with the HIPAA requirements.

Security Awareness and Training

DeVero has implemented a security awareness and training program for all members of its workforce (including management). This includes the following:

Security Reminders
DeVero workforce members are provided periodic security updates.

Protection From Malicious Software
DeVero has implemented procedures for guarding against, detecting, and reporting malicious software.

Login Monitoring
DeVero has implemented procedures for monitoring log-in attempts and reporting discrepancies. DeVero maintains a log of all authentication attempts and is able to track who is making the attempt and when, allowing increased visibility of possible security breaches. DeVero monitors and reviews audit logs to identify any red flags and discrepancies. The logs include all failed login attempts as well as a record of dates and times of previous logins upon the completion of a successful login.

Password Management
DeVero has implemented procedures for creating, changing, and safeguarding passwords. Password management allows DeVero to authenticate any user accessing its service. DeVero has developed policies for appropriately creating, changing, and safeguarding passwords used to verify users' identities and to obtain access to EPHI. DeVero's password management policy includes:

- Requirement of individual passwords to maintain accountability
- Specific requirements to ensure strong passwords
- Mandated password changes every 90 days, where no password can be re-used during a specific period of time
- Symbols are displayed to hide text upon inputting password into EPHI systems
- Secure password distribution to new workforce members and end users

DeVero's authentication processes include:

- Procedures for granting persons and entities authentication credentials or for changing an existing authentication method
- Uniquely identifiable authentication credentials in order to track the identifier to an individual user
- Swift removal or the disabling of authentication credentials in EPHI systems for persons or entities that no longer require access to EPHI
- Protection of authentication credentials with appropriate controls to prevent unauthorized access
- Masking, suppressing, or otherwise obscuring the passwords of persons and entities seeking to access EPHI so that unauthorized persons are not able to view them

Security Incident Procedures

DeVero implements policies and procedures to address security incidents.

Contingency Plan

DeVero has established policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI. Included within this are the following:

Data Backup Plan

DeVero has established and implemented procedures to create and maintain retrievable exact copies of EPHI. Using the Amazon Relational Database Service (Amazon RDS), DeVero makes use of automated backups, and real-time data replication to ensure there are multiple exact copies of the EPHI. Automated full database backups are performed nightly and stored in Amazon RDS. Real-time data replication using Amazon RDS provisions and manages a "standby" database replica in a different AWS Availability Zone (independent infrastructure in a physically separate location).

Disaster Recovery Plan

DeVero has established (and implemented as needed) procedures to restore any loss of data. In the case of a catastrophic failure, DeVero has the ability to do point-in-time restore to any point in the retention period up to the last five minutes. Due to the use of real-time replication using geographically disparate, fault tolerant availability zones, DeVero can fail over to any one of these availability zones should a catastrophic failure occur.

Emergency Mode Operation Plan

DeVero has established (and implemented as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.

Testing and Revisions Procedures

DeVero has implemented procedures for periodic testing and revision of contingency plans.

Applications and Data Criticality Analysis
DeVero assesses the relative criticality of specific applications and data in support of other Contingency Plan components.

Evaluation

DeVero perform periodic technical and non-technical evaluations, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI that establishes the extent to which a covered DeVero's security policies and procedures meet the HIPAA requirements.

Technical Safeguards

DeVero provides HIPAA-compliant technical safeguards that implement the necessary technology and the policy and procedures for its use that protect EPHI and control access to it. These technical safeguards include:

Access Control - technical policies and procedures that allow only authorized persons to access EPHI

Audit Controls - hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use EPHI

Integrity Controls - policies and procedures to ensure that EPHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that EPHI has not been improperly altered or destroyed

Person or Entity Authentication - procedures to verify that a person or entity seeking access to EPHI is the one claimed

Transmission Security - technical security measures that guard against unauthorized access to EPHI that is being transmitted over an electronic network

DeVero's related policies and procedures are described below.

Access Control

Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum necessary information needed to perform job functions. Rights and/or privileges should be granted to authorized users based on a set of access rules.

DeVero has implemented technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.

The following specifications are part of Access Control:

Unique user identification
DeVero requires each user to be assigned a unique name and/or number for identifying and tracking the user's identity. DeVero takes measurable steps to ensure that access to EPHI systems is only granted to members using unique user identifiers (i.e., user IDs) that:

- Identify individual users (i.e., no redundant user IDs)
- Permit activities performed on EPHI systems to be traced to the individual user through the unique ID

Emergency access procedure
DeVero has established (and implemented as needed) procedures for obtaining necessary EPHI during an emergency. DeVero's emergency access procedure delineates the necessary steps to enable authorized users to obtain access to necessary EPHI during a disaster or other emergency including providing all appropriate workforce members with periodic training, documented process materials, and awareness on the emergency access procedure.

Automatic logoff
DeVero has implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity. After a period of inactivity, users will be logged out of EPHI systems. Users will then be required to authenticate in order to regain access and continue the session.

Encryption and decryption
DeVero has implemented a mechanism to encrypt and decrypt EPHI. All data "in-flight" is transmitted via HTTPS/SSL (High-grade Encryption - Camellia-256, 256 bit keys/SHA-1 certificate). For high-risk EPHI, an SHA1 encryption mechanism is used to ensure the integrity of data at rest.

Audit Controls
DeVero's software records and can be used to examine activity in information systems that contain or use EPHI.

Integrity
DeVero protects EPHI in its possession from improper alteration or destruction through the use of policies, procedures and electronic mechanisms. DeVero software can be used to corroborate that EPHI is not altered or destroyed in an unauthorized manner.

Person or Entity Authentication
DeVero utilizes appropriate authentication methods to confirm that only properly authenticated and authorized persons or entities access EPHI. Appropriate access methods are addressed above in the Password Management section above.

Transmission Security, Integrity Controls, Encryption
DeVero utilizes integrity controls to ensure that the value and state of its EPHI is maintained during transmission and that EPHI is protected against unauthorized alteration or destruction during transmission over electronic communications networks. Encryption policies and standards are detailed in the Encryption and Decryption section above.

Physical Safeguards

Physical safeguards include the physical measures, policies, and procedures to protect electronic systems that house EPHI and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

All EPHI provided to DeVero is stored in highly-secure Amazon Web Services (AWS) data centers. Professional AWS security staff tightly control physical access to these centers, utilizing video surveillance and state-of-the-art intrusion detection systems among other state of the art technology. To enter the data centers, authorized staff must pass two-factor authentication at least three times. Access is granted only for those members that have a legitimate business justification. All physical and electronic access to data centers is logged and audited routinely.

Physical Safeguards include the following policies and procedures:

Facility Access Controls

DeVero has implemented policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Workstation Use

DeVero has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.

Workstation Security

DeVero has implemented physical safeguards for all workstations that access EPHI, to restrict access to authorized users.

Device and Media Controls

DeVero has implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI, into and out of a facility, and the movement of these items within the facility.

World-Class Protection via AWS

DeVero's solution is hosted in the Amazon Web Services (AWS) cloud. With the AWS cloud, not only are infrastructure headaches removed, but so are many of the security issues that come with them. AWS's world-class, highly secure data centers utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations. And multiple geographic regions and Availability Zones allow DeVero's service to remain resilient in the face of most failure modes, including natural disasters or system failures.

The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and segregation. For a complete list of all the security measures built into the core AWS cloud infrastructure, platforms, and services, please read the AWS Overview of Security Processes whitepaper available on the AWS website.

Built-in Security Features

Not only is DeVero's service and data protected by highly secure facilities and infrastructure, but they're also protected by extensive network and security monitoring systems. These systems provide basic but important security measures such as distributed denial of service (DDoS) protection and password brute-force detection on AWS Accounts. Additional security measures include:

Secure access – Customer access points, also called API endpoints, allow secure HTTP access (HTTPS) so that secure communication sessions can be established with DeVero's AWS services using SSL/TLS.

Built-in firewalls – DeVero can control how accessible its instances are by configuring built-in firewall rules – from totally public to completely private, or somewhere in between.

Unique users – The AWS Identity and Access Management (IAM) tool allows DeVero to control the level of access its own users have to its AWS infrastructure services. With AWS IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.

Multi-factor authentication (MFA) – AWS provides built-in support for multi-factor authentication (MFA) for use with DeVero's root AWS Account as well as individual IAM user accounts under it.

Encrypted data storage – The data and objects stored in Amazon EBS, Amazon S3, and Amazon RDS are encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.

Security logs – AWS CloudTrail provides logs of all user activity within DeVero's AWS account. DeVero can see what actions were performed on each of its AWS resources and by whom. The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.

Trusted Advisor – Provided automatically when signed up for premium support, the Trusted Advisor service is a convenient way for DeVero to see where it could use a little more security. It monitors AWS resources and alerts DeVero to security configuration gaps such as overly permissive access to certain EC2 instance ports and S3 storage buckets, minimal use of role segregation using IAM, and weak password policies.

Because the AWS cloud infrastructure provides so many built-in security features, DeVero can simply focus on the security of its guest OS and applications. AWS security engineers and solution architects have developed whitepapers and operational checklists to help DeVero select the best options for its needs and recommend security best practices, such as storing secret keys and passwords in a secure manner and rotating or changing them frequently.

AWS Certifications

AWS has achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). AWS undergoes annual SOC 1 audits and has been successfully evaluated at the Moderate level for Federal government systems as well as DIACAP Level 2 for DoD systems.

Each certification means that an auditor has verified that specific security controls are in place and operating as intended. Below is a summary of the certifications and compliance reports available from AWS:

- SOC 1 Report
- SOC 2 Security and Availability Report
- SOC 3 Security Report
- ISO 9001 certification
- ISO 27001 certification
- PCI DSS certification
- DoD CSM Level 3-5 Provisional Authorization
- FedRAMP Compliant Cloud Service Provider

HITRUST Certification

Independent 3rd-Party Audit

DeVero engaged Coalfire Systems, Inc. ("Coalfire"), an accredited HITRUST CSF Assessor, to provide compliance and advisory services and to conduct an assessment of the control processes in place to achieve HITRUST Certification. The overall objective of this project was to assess the DeVero ePHI environment with the requirements identified by the HITRUST CSF, and, notwithstanding any significant control weaknesses, provide necessary evidence to HITRUST for certification. As such, Coalfire's intentions were to validate the design and effectiveness of the controls required for HITRUST certification, as well as HIPAA compliance.

Audit Scope

The scope of the assessment was limited to the DeVero ePHI application and the infrastructure used to create, maintain, receive, and/or transmit customer ePHI. This not only includes the databases, applications, and servers where the data is located; however, also the ancillary environment used to maintain the overall confidentiality, integrity, and availability of the ePHI. This includes firewalls, intrusion detection/prevention systems, as well as the administrative policies and procedures. Coalfire, as part of this assessment, collaborated with DeVero personnel to understand and define the specific systems used to support the DeVero application. Several individuals within the technology department, as well as management personnel, were interviewed for this point-in-time assessment.

About HITRUST

The foundation of all HITRUST programs and services is the HITRUST Common Security Framework (CSF), a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management.
Developed in collaboration with healthcare and information security professionals, the HITRUST CSF rationalizes healthcare-relevant regulations and standards into a single overarching security framework. Because the HITRUST CSF is both risk- and compliance-based, organizations can tailor the security control baselines based on a variety of factors including organization type, size, systems, and regulatory requirements.

The HITRUST CSF is the most widely adopted security framework in the United States healthcare industry. With the inclusion of federal and state regulations, standards, and frameworks such as HIPAA, NIST, ISO, and COBIT, the CSF is a comprehensive and flexible framework that remains sufficiently prescriptive in how control requirements can be scaled and tailored for healthcare organizations of varying types and sizes. The CSF contains 19 security control domains that are comprised of 61 control objectives. The domains are represented in the table below:

1. Information Security Policies
2. Laptop Security
3. Mobile Media Security
4. Wireless Security
5. Malware Protection
6. Configuration Management
7. Vulnerability Management
8. Secure Disposal

9. External Breach Protection
10. PHI Transmission Protection
11. Password Management
12. Access Control and Monitoring
13. Remote Access and Authentication Control
14. Training and Awareness
15. Third Party Security Management
16. Incident and Breach Response
17. Business Continuity/Disaster Recovery
18. Risk Management
19. Physical and Environmental Security

About the Cloud Security Alliance (CSA)

In addition, Coalfire utilized the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire v1.1 that focuses on the key areas noted below. These topics are provided for informational purposes as the topics are incorporated into the HITRUST Common Health Information Protection Questionnaire (CHIP-Q). Many of the risks frequently associated with cloud computing are not new, and can be found in enterprises today. Well planned risk management activities will be crucial in ensuring that information is simultaneously available and protected. Business processes and procedures need to account for security, and information security managers may need to adjust their enterprise's policies and procedures to meet the business's needs. Given the dynamic business environment and focus on globalization, very few enterprises do not outsource some part of their business. Engaging in a relationship with a third party will mean that the business is not only using the services and technology of the cloud provider; but also must deal with the way the provider runs its organization, the architecture the provider has in place, and the provider's organizational culture and policies.

1. Compliance
2. Data Governance
3. Facility Security
4. Human Resource Security
5. Information Security
6. Legal
7. Operations Management
8. Risk Management
9. Release Management
10. Resiliency
11. Security Architecture

HITRUST Certification Granted to DeVero

The objective of Coalfire's engagement was to review the design and effectiveness of the DeVero ePHI control environment with respect to the HITRUST CSF, and to achieve HITRUST certification. In reference to the design of controls, Coalfire believes that DeVero's IT security posture meets the objectives identified by HITRUST, as well those IT security-related requirements identified under the HIPAA Security Rule and HITECH. Coalfire also believes, through detailed audit and control testing, that the ePHI control environment has been adequately designed and that the controls in place are operating effectively. Perhaps most importantly, Coalfire confirmed that the security practices in place at DeVero are commensurate with the overall size, complexity, and level of risk of the organization. Though a limited number of low-risk compliance testing exceptions were noted, they have all been remediated as of the date of this report, and in Coalfire's opinion, meet the HITRUST and HIPAA/HITECH objectives. Coalfire's opinion is based upon DeVero's written and verbal assertions, and Coalfire's tests of compliance during the audit period.