**enterprisehealth**

# MEDICAL INFORMATICS ENGINEERING, INC. DBA ENTERPRISE HEALTH

## System and Organization Controls (SOC 3) Report

## Report on Enterprise Health's System Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy

## Throughout the Period
## February 1, 2021 to January 31, 2022

**AICPA
SOC**
aicpa.org/soc4so
SOC for Service Organizations™

## TABLE OF CONTENTS

# INDEPENDENT SERVICE AUDITOR'S REPORT

## INDEPENDENT SERVICE AUDITOR'S REPORT

To: Management of Medical Informatics Engineering Inc.

### Scope

We have examined Medical Informatics Engineering Inc. dba Enterprise Health's (Enterprise Health) accompanying assertion titled "Assertion of Management of Medical Informatics Engineering Inc. dba Enterprise Health" (assertion) that the controls within Enterprise Health's Data Center, Network Operations Center, and Application Development system (system) were effective throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Enterprise Health uses a subservice organization to provide data center and disaster recovery services. The description of the boundaries of the system (Attachment A) indicates that Enterprise Health's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if subservice organization controls assumed in the design of Enterprise Health's controls are suitably designed and operating effectively, along with related controls at the service organization. The description of the boundaries of the system presents Enterprise Health's system and the types of controls that the service organization assumes have been suitably designed, implemented, and operating effectively at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description of the boundaries of the system (Attachment A) also indicates that Enterprise Health's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Enterprise Health's controls are suitably designed and operating effectively, along with related controls at the service organization. The description of the boundaries of the system presents Enterprise Health's system and the complementary user entity controls assumed in the design of Enterprise Health's controls. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

### Service Organization's Responsibilities

Enterprise Health is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved. Enterprise Health has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Enterprise Health is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

**Service Auditor's Responsibilities**

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Enterprise Health's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Enterprise Health's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

**Inherent Limitations**

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

**Opinion**

In our opinion, management's assertion that the controls within Enterprise Health's Data Center, Network Operations Center, and Application Development system were effective throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if the subservice organization and user entity controls assumed in the design of Enterprise Health's controls operated effectively.

*ControlCase CPA Services*

Arlington, Virginia
April 12, 2022

# ENTERPRISE HEALTH'S ASSERTION

**Assertion of Management of Medical Informatics Engineering, Inc.**
**dba Enterprise Health**

We are responsible for designing, implementing, operating, and maintaining effective controls within Medical Informatics Engineering, Inc. dba Enterprise Health's (Enterprise Health) Data Center, Network Operations Center, and Application Development system (system) throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that Enterprise Health's service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.
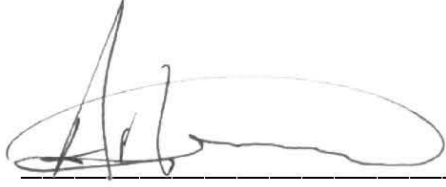
Enterprise Health uses a subservice organization to provide data center and disaster recovery services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Enterprise Health, to achieve Enterprise Health's service commitments and system requirements based on the applicable trust services criteria. The description presents Enterprise Health's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Enterprise Health's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Enterprise Health, to achieve Enterprise Health's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Enterprise Health's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period February 1, 2021, to January 31, 2022, to provide reasonable assurance that Enterprise Health's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signature

 Andrew Horner

Name

 CIO

Title

# ATTACHMENT A

# ENTERPRISE HEALTH'S DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

## ATTACHMENT A – DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

### COMPANY OVERVIEW

Medical Informatics Engineering, Inc. (MIE) is a privately held corporation founded in 1995 to provide health information technology services to healthcare providers, consumers, and employers. MIE aggregated two-plus decades of clinical information management experience, digital consumer engagement expertise, interoperability know-how, and occupational health and compliance capability to develop web-based health information technology.

MIE's operating entities include Enterprise Health. The Enterprise Health IT solution combines occupational health and compliance, clinical care, and employee engagement on a single, interoperable, cloud-based platform.

### DESCRIPTION OF ENTERPRISE HEALTH SERVICES PROVIDED

MIE operates a business unit known as Enterprise Health. This business unit markets health IT applications to large employers, health systems, and government entities who operate their own employee health clinics to meet their occupational health and compliance needs.

Enterprise Health monitors the security and availability of the data center infrastructure and the Enterprise Health application.

More information about the Enterprise Health organization and a description of services can be found at https://www.enterprisehealth.com.

### ENTERPRISE HEALTH SYSTEM BOUNDARIES

Based on the criteria set forth in paragraph 1.04 of the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®) (description criteria), a system is designed, implemented, and operated to achieve specific business objectives (for example, delivery services, production of goods) in accordance with management-specified requirements.

This report addresses the following five components of the Enterprise Health System, which comprise the boundaries of the system:

- Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
- Software. The application programs and IT system software that supports application programs (operating systems, middleware, and utilities).
- People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
- Processes and Procedures. The automated and manual procedures.
- Data. Transaction streams, files, databases, tables, and output are used or processed by a system.

## INFRASTRUCTURE

### Network Zones

The architecture and infrastructure of the Enterprise Health network are designed and maintained in such a way as to ensure that security and availability are being sustained. The storage, processing, and retrieval of client data and Enterprise Health corporate data are segregated into different zones.
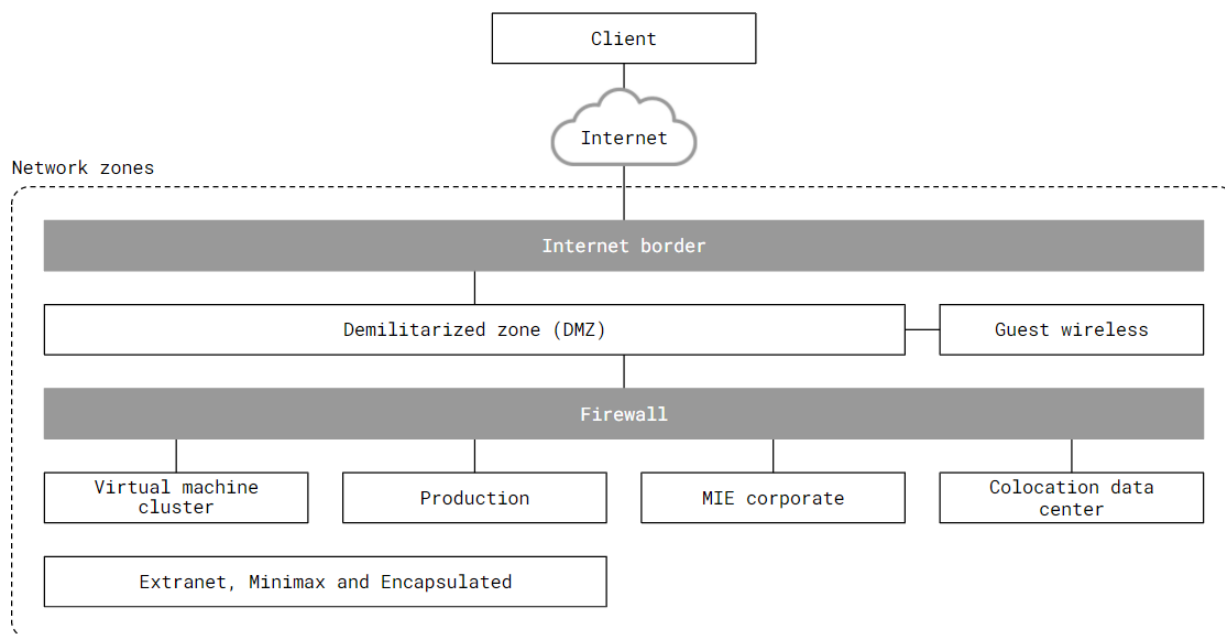


### Internet border

This is our perimeter to the Internet, as well as our first-line defense against intruders. A firewall is located here, along with security monitoring and active defense countermeasures.

### DMZ

Demilitarized zone shared environment, for our own equipment that does not contain PHI, as well as client-owned machines that need internet access.

### Guest Wireless

Restricted building wireless access for guests to use while in our office.

### Firewall

Our central firewall protects access across the different zones.

### Virtual Machine Cluster

A hosting zone where virtual machines are housed. These machines can be present in any zone, depending on the set configuration in the virtual machine host software.

### Production

Servers and networking to support the Enterprise Health system.

### MIE Corporate

Medical Informatics' private corporate network and internal services.

**Colocation Data Center**
Secondary data center housing Disaster Recovery equipment and a secondary Internet connection to provide failover capabilities

## SOFTWARE

The Enterprise Health system is a web-based Software as a Service (SaaS) electronic health record developed and maintained by Enterprise Health's in-house software engineering group. The application is built on the following stack:

- Linux – operating system
- Apache – HTTP server
- MySql (or MariaDB) – relational database management system
- C – programming language

The application supports all major browsers, including Internet Explorer, Edge, Chrome, Firefox, Safari, Opera, as well as other up-to-date browsers.

Enterprise Health is accessible on any mobile device with a browser connected to the Internet. Enterprise Health is mobile optimized and detects the use of a pocket-sized device and optimizes the display of the content for use with these devices.

## PEOPLE

Operations are under the direction of the Chief Executive Officer. Enterprise Health is organized into the following four functional groups:

- Board of Directors

  The Board oversees the organization. The Board is made up of members who are independent of management and meetings are held at least quarterly to review internal control performance. The Enterprise Health Board of Directors is governed by documented bylaws. The Board meets regularly, and the agenda may include Audit Committee updates, the approval of policies, discussion of business operations, and financial updates.

  The Enterprise Health Audit Committee is governed by a documented charter. The Audit Committee meets regularly, and the agenda may include managing the external auditor and reviewing and monitoring audit reports concentrating on financial and information technology controls.

- Corporate Administration

  The CEO is responsible for overseeing strategic financial planning and corporate policy formulation. Administrative responsibilities include oversight of technology resources and service delivery performance and ensuring that these functional areas support the strategic goals and objectives of Enterprise Health. The President coordinates marketing, sales, and account management efforts and oversees new service offering planning.

- Information Technology

  The CIO, utilizing departmental supervisors and subject matter technical staff, manages the following functions:

  - Creation and update of Information Security related to policies and procedures
  - Technology selection and procurement
  - Systems infrastructure security design

  In addition, the CIO supervises staff responsible for monitoring network security, availability, processing integrity, confidentiality, and privacy, and is an integral member of the computer operations, disaster declaration support, and security and technology maintenance teams.

- Product Deployment
  Product deployment teams are responsible for the stand-up, configuration, training, and ongoing support of client environments. This team includes deployment consultants, deployment specialists, and project managers. This area is managed by the Chief Knowledge Officer and the Account Management Director.

- Application Development
  The web application development teams adhere to a rigorous software development life cycle in order to develop quality software that provides an exceptional user experience, has extensive functionality, and safeguards client data based on confidentiality, integrity, and availability. This area is managed by the CTO.

- Legal and Regulatory
  Enterprise Health engages with outside counsel for general compliance, legal, and legislative requirements. To stay up to date with HIPAA regulations, Enterprise Health has engaged with the Tri-State Medical Group, LLC for HIPAA privacy and security support services. The firm assists with documenting HIPAA compliant policies and procedures and conducts HIPAA security audits.

## POLICIES AND PROCEDURES

Enterprise Health has documented policies and procedures to support the operation and controls over the system, available to personnel on MIE's intranet site. Specific examples of the relevant policies and procedures include the following:

- Acceptable Use Policy
  - Two-Factor Authentication Procedure
  - Remote Access Standard
  - Social Media Playbook
- Access Control Policy
  - User Account Provisioning Procedure
- Asset Management Policy
  - Asset Management Procedure
- Business Continuity Management Policy

- o Business Continuity Plan

  o Disaster Recovery Plan

  o Business Impact Analysis

- Change Management Policy

  o Software Development Life Cycle
  o Software Quality Process

  o Release Strategy

  o Data Center Change Control Procedure

  o Server Configuration Standard

  o Firewall Standard

- Clean Desk Policy

- Data Center Security Policy

  o Data Center Access Procedure

  o Media Destruction and Repurposing Procedure

- Data Classification Policy

- Electronic Prescriptions for Controlled Substances (EPCS) Policy

- Encryption Policy

  o Encryption Standard

- Incident Response Policy

  o Incident Response Plan

  o Logging and Monitoring Procedure

- Information Security Awareness

- Information Security Plan

- Information Security Risk Assessment Policy

  o InfoSec Risk Analysis and Management Plan

- Password Policy

  o Password Construction Standard

- Physical Security Policy

  o Physical Access Fob Setup Procedure

  o YubiKey Provisioning Procedure

  o Employee Entry/Exit Procedure

  o Visitor Procedure

- Records Retention Policy

  o Records Retention Schedule

- Security Audit Logging Policy

- Time Synchronization Policy

    o Time Synchronization Procedure

- Vulnerability and Patch Management Policy

    o Vulnerability and Patch Management Procedure

- Wireless Communication Policy

    o Wireless Management Standard

    o Rogue Access Point Procedure

Additional supporting documentation includes:

- HIPAA Privacy & Security Policies

- HIPAA Security Rules – MIE Compliance

- Enterprise Health Privacy Policy

- EU-US and Swiss-US Privacy Shield Policy

- Master Services Agreement

- Employee Handbook

## CLASSIFICATION OF DATA

This component of the system definition is limited to the information used and supported by the system for the purpose of the Enterprise Health System outlined in this description. Enterprise Health is responsible for ensuring the security and availability of data within the Enterprise Health System.

The Enterprise Health application is accessed by users via a secured website using the (TLS) encryption protocol or Virtual Private Network (VPN). User entities are restricted to viewing data within their own unique database and are responsible for administering user access privileges to the web application to authorized personnel. Data is directly input into the electronic health record by the customer via manual input, device interfaces, or electronic interface files. Before data is accepted by the Enterprise Health application, the input data is inspected and validated to ensure appropriate characteristics and quality. The application checks for valid business, syntax, and semantic rules, including character set, length, numerical range, and acceptable values. The system verifies that inputs match specified definitions for format and content. Records of input data are maintained and available to customers via audit logs.

Data in the application consists of PHI and PII and is stored within either a MySQL or MariaDB relational database management system unique to each customer. The application has robust reporting capabilities, including a data visualization platform. All transactions (data updates, report generations, data viewed, and system connections) are logged at a click-level and the logs can be audited by client users with appropriate security privileges. Online support documentation is available to customers regarding data input and output procedures, services, and reporting capabilities.

## COMPLEMENTARY USER ENTITY CONTROLS

This section highlights the internal control responsibilities that Enterprise Health believes should be present at user entities and considered in developing its control objectives described in this report. For user entities to rely on controls reported herein, each user entity must evaluate its own internal controls to determine if the following procedures are in place. The following list of activities is intended to address those controls surrounding the interaction between each user entity and Enterprise Health. These control activities, when coupled with the control activities at Enterprise Health, were designed to achieve the control objectives specified by Enterprise Health's management. Accordingly, this list does not purport to be, and is not, a complete list of the control activities that provide a basis for the assertions underlying the trust services criteria of user entities.

User entities are responsible for the following:

1. User entities are responsible for understanding and complying with their contractual obligations to Enterprise Health (CC2.2, CC2.3).

2. User entities are responsible for notifying Enterprise Health of changes made to technical or administrative contact information (CC2.2, CC2.3).

3. User entities are responsible for ensuring the supervision, management, and control of the use of Enterprise Health's services by their personnel (CC1.5).

4. User entities are responsible for maintaining hardware and software currency on the information assets they own, e.g., firewalls, routers, servers, workstations, applications, browsers, operating systems, and antivirus software (CC6.1).

5. User entities are responsible for notifying Enterprise Health in the event of any compromise of information, control, credentials, or other matter that may affect the security of the Enterprise Health system (CC2.3, CC4.2, P6.3, P6.6).

6. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Enterprise Health's services (CC7.2, CC9.1, A1.2, A1.3).

7. User entities are responsible for ensuring that user IDs and passwords are assigned to only authorized individuals and for provisioning access and revocation of access (CC6.2).

8. User entities are responsible for ensuring that data submitted to Enterprise Health is complete, accurate, and timely (P5.2, P7.1, PI1.1, PI1.2).

9. User entities are responsible for notifying Enterprise Health of issues encountered during the use of Enterprise Health services so that issues can be addressed per contract/service level agreement requirements (CC2.3, PI1.3).

10. User entities are responsible for providing notice and choice regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of

personal information is documented (P1.1, P2.1, P3.1, P3.2, P6.1, P6.2, P6.4, P6.5, P7.1).

11. User entities are responsible for granting and/or denying subjects access to their personal information and for correcting, amending, or appending personal information (P5.1, P5.2, P6.7, P8.1)

## SUBSERVICE ORGANIZATIONS

Enterprise Health utilizes Lifeline Data Centers to provide colocation data center services in Indianapolis, IN. This subservice organization and its controls are excluded from the scope of this examination and report. Enterprise Health monitors Lifeline's controls through the annual third-party vendor assessment and review of Lifeline's SOC 2 report.

- Enterprise Health's hardware and our client's data are securely stored in a dedicated cage in the Lifeline data center.
- Lifeline maintains the following certifications: ISO 27001, NIST 800-53, and a SOC 2 Type 2 report.
- Website link: https://lifelinedatacenters.com/

The following table includes the Complementary Subservice Organization Controls (CSOCs) and the related trust services criteria that Enterprise Health assumes, in the design of its system, will be implemented by the subservice organization and are necessary to achieve the control objectives stated in management's description of the system.

| Principle | Relevant Trust Service Criteria | Complementary Subservice Organizations Controls (CSOCs) |
|---|---|---|
| **Security** | CC6.4 | Lifeline Data Centers are responsible for restricting access to facilities housing the production systems to authorized individuals. |
| **Availability** | A1.2 | Lifeline Data Centers are responsible for environmental protection. |

# ATTACHMENT B

# ENTERPRISE HEALTH'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

## ATTACHMENT B – PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Enterprise Health designs its processes and procedures related to the Enterprise Health System to meet its objectives. Those objectives are based on the service commitments that Enterprise Health makes to user entities, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Enterprise Health has established for the services. The Enterprise Health services are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act, including relevant regulations, as well as state, federal, and international laws, and regulations. Enterprise Health has operational procedures in place to help ensure that customer data security, availability, processing integrity, confidentiality, and privacy commitments can be met. Enterprise Health's commitments to user entities are documented and communicated to customers in master service agreements and the service level addendum. Standard security, availability, processing integrity, confidentiality, and privacy commitments include, but are not limited to, the following:

- Provide information security measures and system availability.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Customer information will not be disclosed to third parties.

Enterprise Health offers three internal hosting options to meet the system objectives of service commitments and system requirements.