Midmark® Smart View™ Limited Release – Cybersecurity

Ensuring the safety and privacy of data is of the highest priority at Midmark. This document applies to all Midmark solutions with Midmark Smart View.

Midmark cloud-connected products incorporate industry best-practice and regulatory compliance controls to secure customer data, including data subject to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and other data that includes Personally Identifiable Information (PII).

With regular data backups, robust application security, penetration testing, data encryption (at rest and in transit) and third-party security assessments, Midmark customers can be assured that data are secured to the highest extent possible.

FREQUENTLY ASKED SECURITY QUESTIONS

What data does Midmark store?

Based on the Midmark Smart View plan, the types of data stored in the cloud depend upon the solution set purchased by the customer.

NOTE: The following examples cover the most common solutions. Customer-specific use cases may vary based on configuration.

NOTE: No Personal Health Information (PHI) or Personally Identifiable Information (PII) is collected by Midmark.

The following data could be collected depending on the device:

- Telemetry from Device
  - Temperature
  - Voltage
  - Current
  - Etc.
- Asset Data
  - Asset identifiers (ID, display name, serial number)
  - Asset descriptors [manufacturer (i.e., Midmark), model, department/unit location]
  - Preventive maintenance date
  - Etc.
- Software and Configuration Data (including Firmware version)

Where are the data stored?

Data are securely stored with Microsoft® Azure®, the primary cloud infrastructure provider for Midmark. All data are primarily stored in the Azure East or Central US regions located in Virginia, United States. A secondary data center for geo-replication is the Azure West US region located in California, United States. The data repositories within the cloud environment can be SQL databases or blob storage resources.

Does Midmark participate in customer security reviews/assessments?

Yes, Midmark will participate in customer security reviews. To streamline the review process, Midmark provides this document to facilitate answers to common questions relative to the corporation's commitment to security. The intent of this document is to be transparent on our approach to a variety of security topics.

Does Midmark conduct third-party security assessments?

Yes, all Midmark cloud products and solutions are subject to third-party security testing. The goal for Midmark is to integrate security as a core feature, so assessments are incorporated during design and new product development. Ongoing assessments are conducted annually, or when key product architecture is changed. The assessment firms use industry standards, including OWASP, NIST, PTES, and OSSTMM, as a baseline for testing.

Midmark® Smart View™ Limited Release – Cybersecurity

Does Midmark have a cybersecurity team?

Midmark has multiple cybersecurity teams and personnel across the organization. The Midmark Cybersecurity Council and the Midmark Cybersecurity Management Team define and govern cybersecurity strategy across all Midmark products.

SECURITY FEATURES

Single Sign-On + Identity Federation

Midmark recognizes the importance of centrally managing user accounts for both security and convenience. Midmark is committed to developing support for various authentication protocols and currently supports federation with customers' Azure Active Directory.

User Roles + Authentication

Midmark solutions utilize a role-based authorization model, whereby user access to various aspects and functionality of the application are determined by role. Using this model ensures separation of duties and safeguards for data confidentiality and integrity.

Password Management

Midmark password policy for both customer user provisioning and Midmark teammates includes the following requirements:

- Minimum of 10 characters
- Complexity requirements of upper-case, lower-case, numeric and special characters

Geographic Access

Access to Midmark applications, solutions and infrastructure is only allowed from designated and trusted-source geographies. Explicitly limiting inbound connectivity offers another layer of security for customer data.

INFRASTRUCTURE + NETWORK SECURITY

Application Infrastructure

Midmark utilizes best-of-breed application development environments to develop and deploy solutions. With Microsoft Azure Software as a Service (SaaS) and underlying infrastructure, coupled with Azure DevOps for Continuous Integration and Continuous Delivery (CICD) pipeline management, Midmark is equipped to dynamically support the complete application lifecycle: building, testing, deploying, managing, and updating within the same integrated environment.

Access Controls

Midmark follows the principle of least privilege, meaning that only the correct users have access to given resources when needed. Role-based access control delineates access appropriately to maintain confidentiality, integrity and availability.

In addition to role-based access control, users must leverage Multi-Factor Authentication (MFA) to access cloud infrastructure resources.

Vulnerability Management

Midmark leverages vulnerability management policies, processes and procedures to identify vulnerabilities from multiple sources. After identification, these vulnerabilities are managed in accordance with remediation timeframes, based on severity. Sources for vulnerability identification include:

- Application security scanning (SAST, DAST, Software Composition Analysis)
- Third-party security assessments, including penetration testing
- Cloud security services and logging
- Security Information and Event Management (SIEM) tooling
- Vendor disclosure
- Vulnerability databases

Penetration Testing

Midmark conducts third-party security assessments on an annual basis, or more frequently depending on changes in design or integrations. Midmark contracts with industry-leading security assessment firms who perform tests based on best-practice methodologies, including OWASP Security Testing Guides and NIST 800-115. Tests are executed to detect flaws and vulnerabilities in applications, including:

- Injection (SQL, Command, Expression, Server-side template, Hibernate, etc.)
- Authentication
- Authorization
- Sensitive Data Exposure
- XML Configuration
- Access Control
- Misconfiguration / Insecure Configuration

Intrusion Detection + Prevention

Midmark cloud-based solutions have multiple intrusion detection and prevention controls. Security logs are parsed for anomalous activity by a Security Information and Event Management (SIEM) tool. Services are protected by Web Application Firewalls (WAF), designed to protect information and resources by limiting illicit traffic patterns. Azure Distributed Denial-of-Service (DDoS) Protection secures cloud resources from denial of service (DoS) attacks with always-on monitoring and automatic network attack mitigation.

Midmark® Smart View™ Limited Release – Cybersecurity

Logging + Monitoring
Midmark leverages a Security Information and Event Management (SIEM) tool to inspect logs and trigger an event for anomalous activity. Additionally, Midmark cloud services utilize cloud-native security monitoring to notify support teams of suspicious activity within the environment.

Logical Separation
The architecture of Midmark cloud services leverages logical separation by segregating resources that process or store sensitive information. Virtual networks are used to protect sensitive storage resources, and databases are secured with zero-trust firewall rules. Additionally, client data remain independent and separated by using individual database allocation.

Incident Response Plan
The Midmark Incident Response Team follows an established incident response policy to ensure that proper protocol is followed in the event of a security incident.

Vulnerability Disclosure
Midmark vulnerability management policies and procedures include various methods to detect potential vulnerabilities within Midmark products and services. Midmark actively works with third-party vulnerability assessment firms for active identification of vulnerabilities. Additionally, Midmark will publish known product vulnerabilities within respective product documentation and within pertinent Midmark knowledge bases. Alerts and notifications will be provided to customers, along with resources for remediation and support.

Product Development Life Cycle
Midmark has adopted a security "shift-left" strategy to ensure security is organic to the Product Development Life Cycle. During new product development, analysis is performed against industry framework cybersecurity requirements. Subsequently, a Cybersecurity Risk Assessment (CRA) is performed, and product design history is updated and maintained. Developers utilize industry-best SAST and DAST tools to identify code and web application vulnerabilities and remediate them early in software development.

DATA SECURITY

Data Encryption
Protecting client data is paramount. Data at rest within Midmark cloud services are encrypted and decrypted transparently using 256-bit Advanced Encryption Standard (AES) encryption, one of the strongest block ciphers available. Midmark cloud-based offerings are FIPS 140-2 compliant.

Data in transit to and from Midmark cloud services are protected by leveraging Transport Layer Security (TLS) with Perfect Forward Secrecy and RSA-based 2,048-bit encryption key lengths.

Data Retention
Midmark stores client data for 24 months, after which time it is securely destroyed. No additional archiving or data transfer options are currently available. Midmark is committed to serving the data retention and transfer needs of customers and welcomes input.

Data Sub-processors
To support the delivery of cloud-connected products, Midmark uses Microsoft Azure Cloud Computing Services. **https://azure.microsoft.com**

- Location: Redmond, WA, United States
- Security certifications: ISO 27001, SOC3, FIPS 140-2, etc.; more information available: **learn.microsoft.com/en-us/azure/compliance/**
- Data processed: Anonymized content, email address, IP address
- Use: Data storage, compute resources, database services, application services, security services

Data Breach Disclosure
In accordance with governing Business Associate Agreements (BAA) and regulatory requirements, and in alignment with the Midmark Incident Response Policy, Midmark will notify customers of any data breach in a timely manner.

BUSINESS CONTINUITY + DISASTER RECOVERY

High Availability
Midmark has documented availability management policies and processes with stated key performance indicators (KPI) for uptime metrics and targets. Midmark offers technical services from 8:00 AM to 6:00 PM ET, Monday–Thursday and 8:00 AM to 5:00 PM ET on Fridays.

Business Continuity Plan
The Midmark business continuity plan uses Business Impact Analysis (BIA) to identify business-critical operations and appropriate measures to ensure those operations continue in the event of a disruption. Disruption severity, roles and responsibilities, procedures, alternate suppliers, and crisis communication protocols are documented to ensure Midmark products and services provide continued value to our customers.

Disaster Recovery
The Midmark disaster recovery plan includes restoration management with the following prioritization:

- Restore the flow of telemetry to the cloud
- Restore application layer functionality, which includes integrations and visualizations
- Restore customer-specific data storage from backups

Midmark® Smart View™ Limited Release – Cybersecurity

Backups

Midmark cloud services utilize Microsoft SQL Server technology to create full database backups every week, differential backups every 12 to 24 hours and transaction log backups every 5 to 10 minutes. SQL resources store data in geo-redundant storage that is replicated to a paired region. Geo-redundancy helps protect against outages impacting backup storage in the primary region and allows Midmark to restore servers to a different region in the event of a disaster.

Insurance

Midmark carries cybersecurity liability insurance through Allied World Insurance.

MIDMARK CORPORATE SECURITY

Physical Security

Midmark physical access controls include requirements for badged entry to corporate property, surveillance of key entry points, proper signage and segregation of sensitive IT infrastructure equipment.

Endpoint Security

Midmark leverages SentinelOne® for endpoint security as well as advanced VPN software for remote endpoints connecting to the corporate network. Microsoft Comp Portal is used for mobile device management and security.

Security Training

Midmark requires formal HIPAA compliance training and annual cybersecurity training for employees, including requirements to assess and certify completion. Additionally, Midmark teammates are required to take security policy training when relevant to specific job roles and responsibilities.

Risk Management

The Midmark Risk Management Policy sets standards on iterative risk assessment and response, including standardized risk assessment templates and scoring based on the Common Vulnerability Scoring System (CVSS).

Security Policies

The Midmark Cybersecurity Council and the Cybersecurity Management Team are responsible for identifying, drafting and publishing overarching corporate security policies. Security policies include risk management, incident response, cybersecurity framework, data management and many others. All downstream Midmark processes and procedures must comply with security policy requirements.

Vendor Management

Midmark vendor management includes the policies and procedures for standard contract language and terms, risk assessment and mitigation, and engagement lifecycle.

Confidentiality Agreements

Midmark leverages standard Non-Disclosure Agreements (NDA) as well as Business Associate Agreements (BAA), where applicable. The Midmark legal team will work with vendors and customers on specific agreement terms. Customers interested in reviewing further detail regarding confidentiality agreements can contact their Midmark sales representative.

Background Checks

Midmark Human Resources conducts standard background checks, per policy, for employees going through the hiring process.

SECURITY COMPLIANCE

HIPAA

Midmark is continuously and relentlessly focused on protecting customer data, including sensitive Personal Health Information (PHI), as defined by HIPAA. In addition to administrative and technical controls, Midmark conducts annual third-party security assessments to provide an objective review of HIPAA and security compliance posture.

The most recent HIPAA Security Risk Analysis (HSRA) for Business Associates was performed by 4A Security and Compliance, concluding on November 30, 2021, indicating that customers using Midmark cloud products can sustain HIPAA compliance. Please refer to "Appendix 1: HIPAA Attestation Letter," for additional information on the HSRA and its outcome.

SOC 2

Midmark has completed a SOC 2 readiness assessment, demonstrating that Midmark products have the appropriate controls in place to mitigate risks related to security, confidentiality, availability, processing, integrity and privacy.

Security Alliances and Information Sharing and Analysis Organizations (ISAOs)

Midmark is an active member of the Health Information Sharing and Analysis Center (H-ISAC).

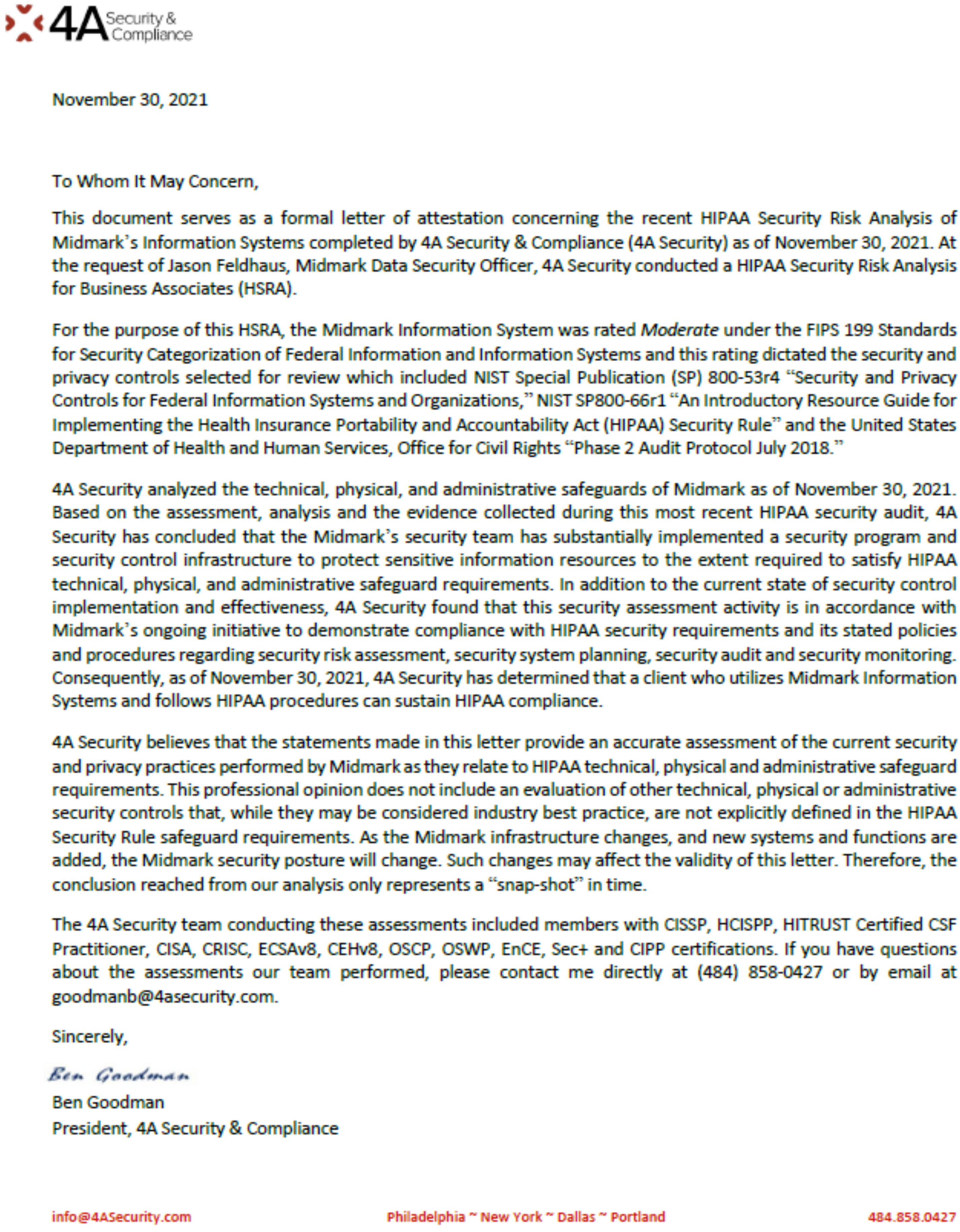
"Health-ISAC Inc. (H-ISAC, Health Information Sharing and Analysis Center), is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating, and sharing vital physical and cyber threat intelligence and best practices with each other."

Security Frameworks

Midmark aligns to industry-leading cybersecurity frameworks to ensure information confidentiality, integrity and availability.

- ISO 27001 – Overarching international standard for managing information security
- National Institute of Standards and Technology (NIST) CSF and 800-53 – Catalog of security and privacy controls covering 18 areas, including access control, incident response, business continuity and disaster recoverability

Microsoft and Azure are registered trademarks of Microsoft Corporation. SentinelOne is a registered trademark of SENTINELONE, INC.



4A Security & Compliance

November 30, 2021

To Whom It May Concern,

This document serves as a formal letter of attestation concerning the recent HIPAA Security Risk Analysis of Midmark's Information Systems completed by 4A Security & Compliance (4A Security) as of November 30, 2021. At the request of Jason Feldhaus, Midmark Data Security Officer, 4A Security conducted a HIPAA Security Risk Analysis for Business Associates (HSRA).

For the purpose of this HSRA, the Midmark Information System was rated *Moderate* under the FIPS 199 Standards for Security Categorization of Federal Information and Information Systems and this rating dictated the security and privacy controls selected for review which included NIST Special Publication (SP) 800-53r4 "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP800-66r1 "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" and the United States Department of Health and Human Services, Office for Civil Rights "Phase 2 Audit Protocol July 2018."

4A Security analyzed the technical, physical, and administrative safeguards of Midmark as of November 30, 2021. Based on the assessment, analysis and the evidence collected during this most recent HIPAA security audit, 4A Security has concluded that the Midmark's security team has substantially implemented a security program and security control infrastructure to protect sensitive information resources to the extent required to satisfy HIPAA technical, physical, and administrative safeguard requirements. In addition to the current state of security control implementation and effectiveness, 4A Security found that this security assessment activity is in accordance with Midmark's ongoing initiative to demonstrate compliance with HIPAA security requirements and its stated policies and procedures regarding security risk assessment, security system planning, security audit and security monitoring. Consequently, as of November 30, 2021, 4A Security has determined that a client who utilizes Midmark Information Systems and follows HIPAA procedures can sustain HIPAA compliance.

4A Security believes that the statements made in this letter provide an accurate assessment of the current security and privacy practices performed by Midmark as they relate to HIPAA technical, physical and administrative safeguard requirements. This professional opinion does not include an evaluation of other technical, physical or administrative security controls that, while they may be considered industry best practice, are not explicitly defined in the HIPAA Security Rule safeguard requirements. As the Midmark infrastructure changes, and new systems and functions are added, the Midmark security posture will change. Such changes may affect the validity of this letter. Therefore, the conclusion reached from our analysis only represents a "snap-shot" in time.

The 4A Security team conducting these assessments included members with CISSP, HCISPP, HITRUST Certified CSF Practitioner, CISA, CRISC, ECSAv8, CEHv8, OSCP, OSWP, EnCE, Sec+ and CIPP certifications. If you have questions about the assessments our team performed, please contact me directly at (484) 858-0427 or by email at goodmanb@4asecurity.com.

Sincerely,

Ben Goodman

Ben Goodman
President, 4A Security & Compliance

info@4ASecurity.com Philadelphia ~ New York ~ Dallas ~ Portland 484.858.0427

CONFIDENTIAL TO MIDMARK TEAMMATES

NOTE: Select dealers are participating in this program. Ask your Midmark sales representative for details.
Products subject to improvement changes without notice. Litho in USA.