Information Security and Privacy White Paper

Version: 2018.4
Date: 5 September 2018
Author: Scott Sumner, Vice President R&D (InfoSec)
Pages: 31

This page intentionally left blank

Table of Contents

Figures

Medidata Information Security and Privacy

Medidata's solutions deliver an entire clinical development process through innovative clinical cloud technology. Whether for your first study or an enterprise solution across multiple phases and therapeutic areas, our suite of products streamlines key clinical development operations, including protocol development, trial planning and management, site collaboration, randomization and trial supply management, monitoring, safety event capture, electronic data capture (EDC) and management, advanced reporting and business analytics. Medidata delivers clinical cloud computing solutions with high availability, integrity, confidentiality, reliability and the flexibility to enable customers to access a wide range of applications. Medidata builds services in accordance with security best practices and provides the appropriate security features to ensure end-to-end security and end-to-end privacy. Ensuring the confidentiality, integrity and availability of customer data is of the highest importance to Medidata, as is maintaining trust and confidence.

Medidata provides a wide range of information regarding its hosted IT environment to customers through a variety of white papers, reports, certifications and third-party attestations. This information assists customers in understanding the controls in place relevant to the Medidata products and services they use and how independent auditors validate those controls. This information also assists customers in their efforts to account for and to validate that controls are operating effectively in their extended IT environment.

Overview

Policy

Information security policy defines what it means for a system, organization or other entity to be secure. At Medidata, it addresses the constraints on behavior of all staff as well as constraints imposed on potential adversaries by mechanisms such as doors, locks, firewalls and scanners. Medidata constrains access by external systems and adversaries including programs and access to data by people. To assure the completeness of our security policies, we follow the ISO 27001 architecture as a baseline, and then supplement this with portions of other recognized security architectures.

Roles and Responsibilities

Medidata has clearly segregated duties, based on business need, for management of the software-as-a-service (SaaS) resources. The following lists the typical resource groups and the tasks for which they are responsible.

1. Technology: The Executive Vice President, Technology and Chief Technology Officer (CTO) is the executive manager of Medidata applications' technical operations. The span of control covers development, operations and information security. This position oversees application management from architecture, engineering, testing and implementation to maintenance. CTO is also responsible for ensuring clients' technical review, pre-assessment and audit requests are addressed.
2. DevOps: This team is comprised of individuals who are dedicated to ensuring the continuous working of Medidata applications.
3. Service Delivery: The service delivery team is comprised of individuals tasked with the installation, configuration, change and maintenance of all hardware-, software- and infrastructure-related activities to support the Medidata applications.

4. Network Operations Center (NOC): The system-monitoring group is responsible for configuring, maintaining and monitoring alerts and notices critical to ensuring the uptime and health of Medidata applications and infrastructure.
5. Information Security: The group headed by the Vice President, R&D (InfoSec) is tasked with the management of policies in the context of publicly accepted standards, regulations and frameworks as well as the implementation of those controls to ensure that the security, scalability and stability of the technical environment is maintained.
6. Enterprise Support: The corporate IT team helps support the enterprise IT services to enable Medidata to operate and conduct its daily business activities. The enterprise support team does not have access to nor any access into customer-facing Medidata applications.

Reports, Certifications and Independent Attestations

In 2011, Medidata successfully completed a Service Organization Controls 2 (SOC 2) report in accordance with the SSAE 16 professional standards. In April 2017, Medidata successfully completed a Service Organization Controls 1 (SOC 1) report for our "Medidata Payments" application. For our United States (U.S.) government clients, Medidata completed our initial FISMA certification and accreditation in 2009. For international clients concerned with privacy, we received authorization in 2011 from the U.S. Department of Commerce to participate in the Safe Harbor program that certifies the protection we afford is equivalent to the protections required in the European Union (EU 95/46). In addition, in November 2016, the U.S. Department of Commerce approved Medidata's self-certification to the Privacy Shield program. Medidata also received an ISO 27001:2013 certification in October 2016, followed by an ISO 27018:204 in July of 2018. We will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our products and services.

Physical Security

Medidata has many years of experience in designing, constructing and operating data centers. Our physical security can best be described as military grade. We employ a combination of building guards, smart-ID badges with electronic access, video surveillance and biometric scanners. Our buildings are non-descript and only those who have a legitimate business need know the actual location of these data centers. Acquisitions noted below scheduled to be absorbed in 2019.

Network Security

Network security is a 24-hour-a-day priority at Medidata. We start with border protection that includes routers and load balancers to provide high availability even during distributed denial of service (DDoS) attacks. Border protection is bolstered by our firewalls that deny all inbound ports with no identified business purpose as well as outbound ports. Authorized data that passes through the firewall is then subjected to a series of malware scanners as well an intrusion detection/prevention system. We scan our networks monthly; and submit our networks to a third-party assessment annually to identify and correct any new Internet vulnerabilities.

Application Security

Medidata's applications are critical to our success and making sure they are safe and secure for our customers is paramount. Consequently, we perform numerous internal tests using WhiteHat on our software during the development process. Then we take our production products and dedicate time for internal hacking (Black Hat). During this phase, we attempt to uncover and then patch subtle issues that are only detectable with an intimate knowledge of our source code. Medidata then goes to the next level by evaluating the interoperability of the product suite to improve the resilience of our products. Medidata also submits our software to third-party assessments to identify and patch any vulnerability that may have made it to this point in the lifecycle. Vulnerabilities discovered during internal or external third-party testing are logged into Medidata's JIRA™ trouble ticketing system. From there our internal teams analyze the vulnerability, confirm it and then estimate a remediation date. The assigned team has ninety (90) days to resolve the request before it is elevated to the CISO for review and possible deadline extension. After ninety (90) days, it also requires the CIO or the COO review and approval for further extensions. Extensions are generally granted for situations where a patch isn't available from a software manufacturer, or where a repair requires extensive development and testing to avoid creating a greater problem upon deployment.

Security of Medidata Applications

Subjected to Threat Modeling

Internal Vulnerability Test	Black Hat Test	Performance Test	External Pen Text
☆	☆	☆	☆
• **Tools** ○ Brakeman ○ BurpSuite Pro ○ Security Center ○ Tenable.io ○ WhiteHat • **Discover** Common threats • **Remediate**	• **Discover** Unique threats • **Remediate** • **Train** Developers	• Survivable applications • Increase reliability	• Independent verification

Figure 1. Application Security

Data Privacy

Medidata treats the privacy of our customers' data as a top priority. Global privacy regulations vary considerably, so our approach is that protecting to the most stringent standards is best. Medidata established a privacy policy and makes it publicly available at http://www.mdsol.com/privacy. We protect the data from workstation to destination using a Transport Layer Security (TLS 1.2) encryption; encryption at rest is in place across the entire environment, using Advanced Encryption Algorithm (256 bit). We review the privacy policies of countries around the world and make sure our controls comply with the most restrictive for data transferred and stored in the U.S. To attest to the efficacy of the controls, we have been self-certified in the EU-US Safe Harbor program since 2011 and in 2016 we joined the replacement for Safe Harbor – Privacy Shield.

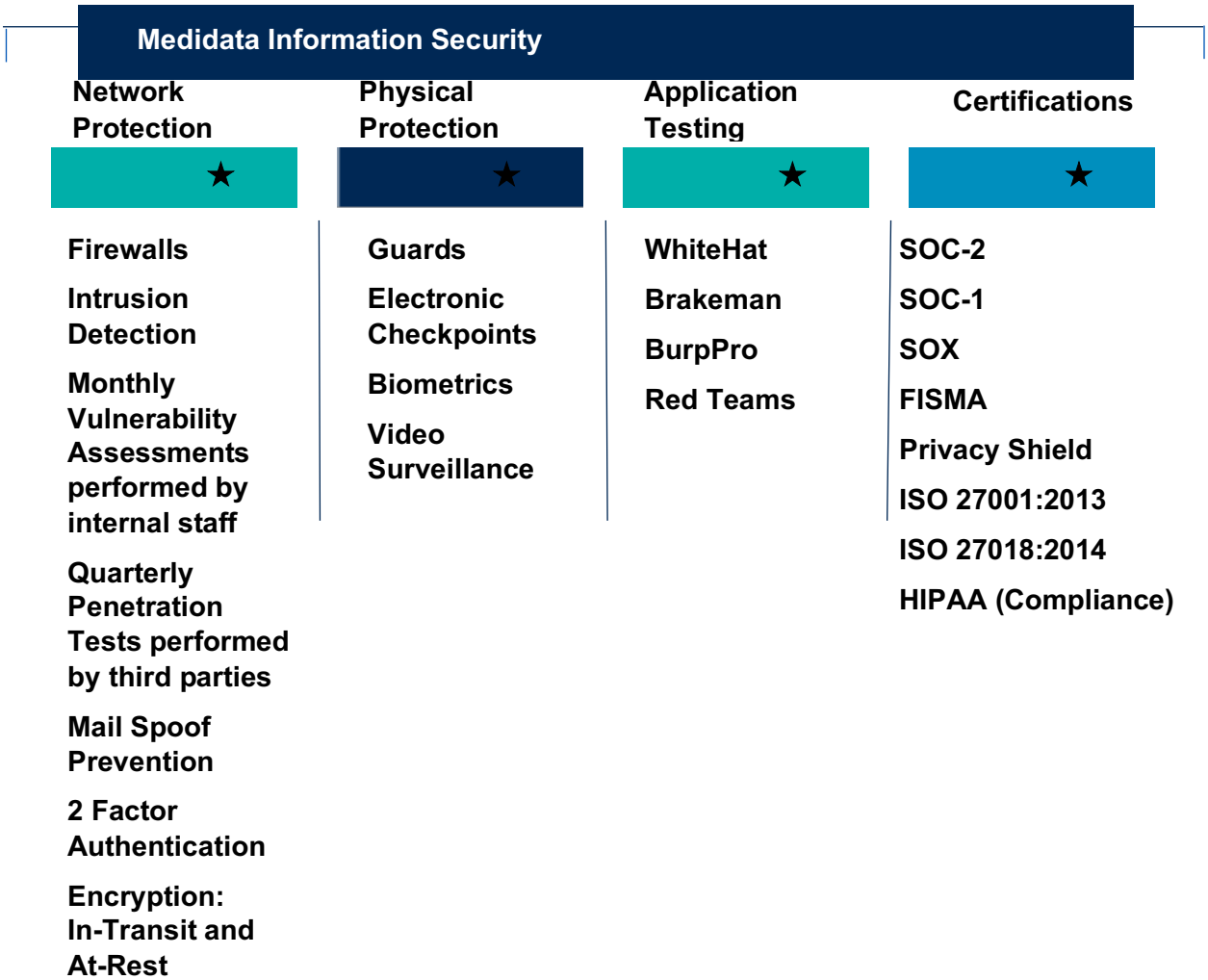


Figure 2. Data Privacy

Certifications and Accreditations

ISO 27001:2013

ISO 27001:2013 is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. This is a widely recognized international security standard in which Medidata clients showed significant interest. Certification in the standard requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet our information security needs on an ongoing basis

The key to certification under this standard is the effective management of a rigorous security program. The Information Security Management System (ISMS) required under this standard defines how we continually manage security in a holistic, comprehensive way. The ISO 27001:2013 certification is specifically focused on the Medidata ISMS and measures how our internal processes follow the ISO standard. Certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms we are operating in alignment with the comprehensive ISO 27001:2013 certification standard.

ISO/IEC 27018:2014

ISO/IEC 27018:2018 is a security management standard that specifies security management best practices and comprehensive security controls in the context of Privacy Information in a cloud environment. This is a widely recognized international security standard in which Medidata clients also show significant interest.

This standard complements ISO/IEC 27001:2013 and other security frameworks in order effective management of a privacy related information. Like ISO/IEC 27001:2013, ISO/IEC 27018:2014 certification means a third party accredited independent auditor has performed an assessment of our processes and controls and confirms we are operating in alignment with the comprehensive ISO 27018:2014 certification standard.

SOC-1 Type 1

Medidata published its first SOC1 Type 1 report for our “Medidata Payments” application in 2017. SOC-1 Type 1 reports are examination engagements performed by a service auditor (CPA) in accordance with Statement on Standards for Attestation Engagements (SSAE) 16, *Reporting on Controls at a Service Organization,* to report on the suitability of the design of the controls at a service organization that are likely to be relevant to an audit of a user entity’s financial statements. **Use of a SOC 1® report is restricted to existing user entities (not potential customers) and their auditors**.

SOC 2 Type 2

Medidata publishes a Service Organization Controls 2 (SOC 2) report. This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report can meet a broad range of auditing requirements for U.S. and international auditing bodies. The SOC 2 report audit attests that Medidata data center control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. Our commitment to the SOC 2 report is ongoing, and we plan to continue our process of periodic audits.

FISMA

Medidata enables U.S. government agency customers to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). FISMA requires federal agencies to develop, document, and implement an information security system for its data and infrastructure based on the National Institute of Standards and Technology Special Publication 800-53, Revision 4 standard. FISMA requires Medidata to implement and operate an extensive set of security configurations and controls. This includes documenting the management, operational and technical processes used to secure the physical and virtual infrastructure, as well as the third-party audit of the established processes and controls. Medidata is evaluated every year to maintain our FISMA compliance for Software as a Service.

Privacy Shield

The EU-U.S. Privacy Shield imposes strong obligations on U.S. companies to protect Europeans' personal data. It reflects the requirements of the European Court of Justice, which ruled the previous Safe Harbor framework invalid. The Privacy Shield requires the U.S. to monitor and enforce more robustly, and cooperate more with European Data Protection Authorities. It includes, for the first time, written commitments and assurance regarding access to data by public authorities.

What will it mean in practice?

- For Medidata Solutions
  - Self-certify annually that we meet the requirements.
  - Display a privacy policy on our website.
  - Reply promptly to any complaints.
  - (If handling human resources data) Cooperate and comply with European Data Protection Authorities.
- For European Clients of Medidata Solutions
  - More transparency about transfers of personal data to the U.S. and stronger protection of personal data.
  - Easier and cheaper redress possibilities in case of complaints —directly or with the help of your local Data Protection Authority.

FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, Medidata Private Cloud VPN endpoints and TLS-terminating load balancers in Medidata (U.S.) operate using FIPS 140-2 validated algorithms. Operating in FIPS-140-2 compliance mode does require comparable capabilities at the user browser side of the connection. While we do not employ FIPS 140-2 certified hardware, we do use the comparable make and model with fully approved FIPS 140-2 software.

PCI DSS Service Provider

The Payment Card Industry Data Security Standard (PCI/DSS) was created to standardize controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually, either by our trained and certified Internal Security Assessor (ISA). We also apply it to any financial processing related information that is used as part of our Payments offering.

HIPAA

Medidata enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure Medidata environment to process, maintain, and store protected health information.

Physical Security

Non-descript buildings

Systems are housed in non-descript buildings that provide no indication that Medidata computers are within.

Uniformed Guards

The buildings we use for most of our data centers have uniformed guards at the entrances checking identification badges. All visitors to Medidata space must wear a visitor nametag and be escorted within the Medidata space. In our Cincinnati location, uniformed guards are not used, but staff can monitor the modest data center at this location.

Photo-ID Smart Cards

Our data centers employ photo-ID cards to gain access to the database server rooms. In addition to being a positive identification tool, these ID cards also operate electronic door access locks. Cincinnati has not been upgraded to photo-ID badge access due to the limited data present at this location.

Biometric Door Locks

Outside of our server room access doors we have a biometric finger scanner that must be used in conjunction with a PIN code and the photo-ID smart card to gain access. Cincinnati does not employ biometric access.

Video Surveillance

Anyone approaching any of our data centers is recorded on a video surveillance system; the video is stored forever as well as constantly monitored by our skilled Network Operations Center staff 24x7.

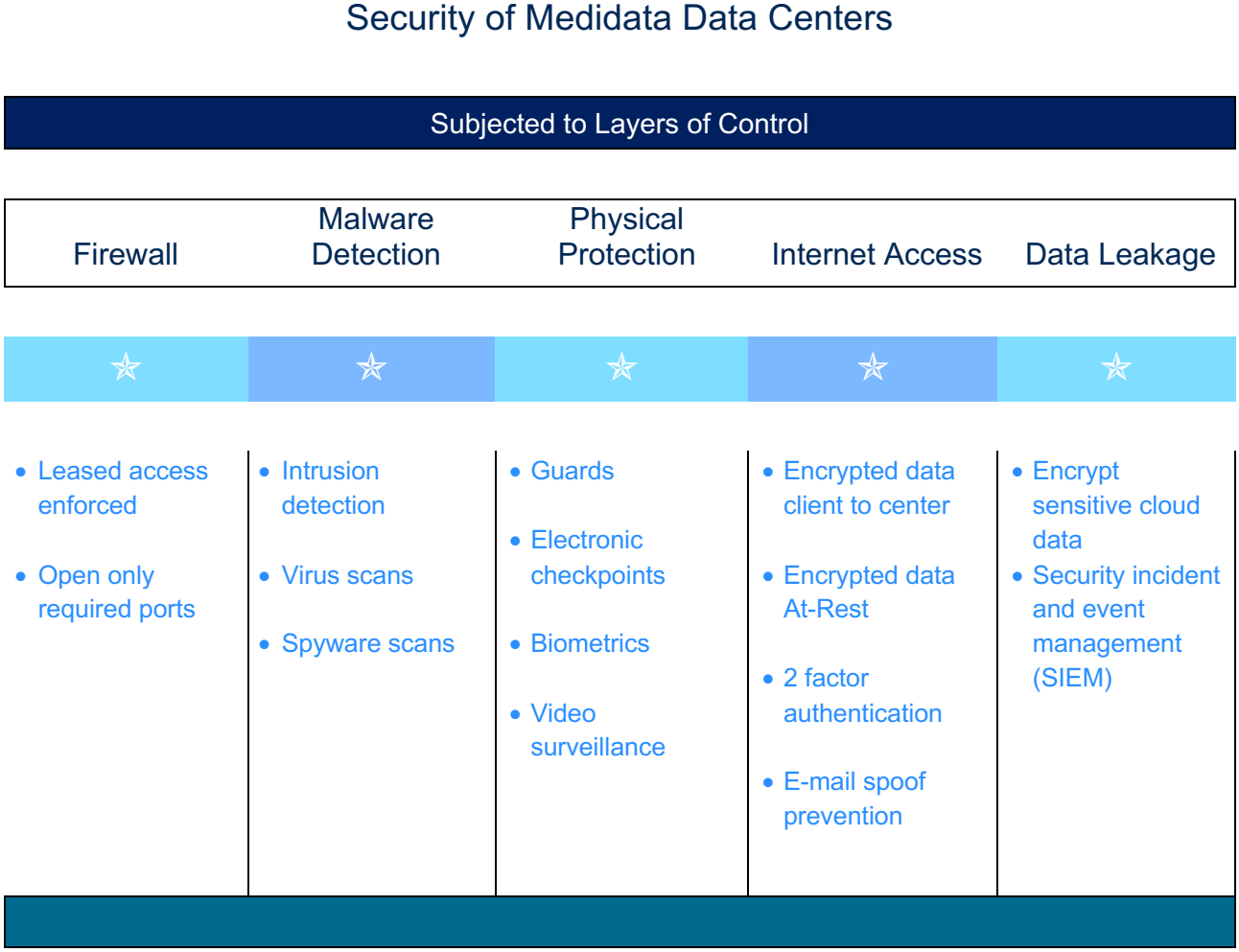


Figure 3. Data Center Security

Network Security

Palo Alto Networks PA 5060 Firewall, Virus Scan, & IDP
Certified: [EAL4+, FIPS 140-2, USGV6, UC APL]

Firewall

Medidata provides a comprehensive firewall solution. The inbound firewalls are configured in a default deny-all mode except for ports 80 (HTTP) and/or port 443 (HTTPS). The outbound firewalls are configured in a default deny-all mode. The firewalls are updated with the most current definitions available on scheduled basis consistent with our change management procedures. Firewalls are configured to provide OSI model layer 2 (Data Link) through layer 7 (Application) security.

Intrusion Detection & Prevention

Medidata's IDS offers protection from both external and internal attackers—where traffic doesn't go past the firewall at all. Our systems use signature analysis mechanisms to analyze all traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. Application and network traffic signature pattern matching is used to identify potential security weaknesses. Protocol anomaly traffic detection analyzes network traffic for known attacks and variations of those attacks. Updated network traffic signature files are automatically implemented upon release by the vendor.

Information Security

Malware

In addition to our IDS and Firewall, Medidata uses a range of scanning tools to further sanitize all data prior to it traversing our data center networks. These scanning tools notify us in the event something malicious has made it through our defenses and may attempt to access our systems. Medidata network security lives by the old saying, “An ounce of prevention is better than a pound of cure.” In this case, a Malware scan is the prevention.

TrendMicro is installed on all Production and Validations systems, including the Anti-Malware, Server Firewall, Log Inspection and Intrusion Detection & Prevention modules.

Security Management

Security Incident and Event Management (SIEM)

- SumoLogic SIEM System collects log and event data from all network devices and performs true real-time correlation and notification 24x7
- Enables Medidata to automatically take action against threats
- Automates security audits using over 120 customizable, out-of-the-box checks based on standards from NSA, NIST and SANS
- Detects data leakage
- Analyzes firewall configurations and logs to isolate redundant and unused rules and objects
- Models how a new rule, or change to an existing one, will impact our firewall policy—without touching production devices
- Scans our inventory for high-risk firewalls and assesses our risk profile in minutes
- Captures audit events:
    - Logon (unsuccessful and successful) and logout (successful)
    - Unauthorized access attempts to files (unsuccessful)
    - Application and session initiation (unsuccessful and successful)
    - System startup and shutdown (unsuccessful and successful)
    - System administration actions
    - Security personnel actions
    - Data transfers (from, to, time, size and correlation to norms for that URL)

Routers

Access Control Lists (ACL) are used and managed to segregate web, application and database servers. Communication between servers is accomplished via an approved ACL address and in conjunction with authentication.

Encryption during Data Transmission

All data is transmitted from the client site through the Internet to one of our data centers located in the continental United States. To maintain the highest level of confidentiality and meet our Privacy Shield requirements, all data is encrypted with at least 256 bits of key strength.

Encryption at Rest

Currently Medidata encrypts data at rest for its Rave, RaveX, Insights, Safety Gateway and Coder applications

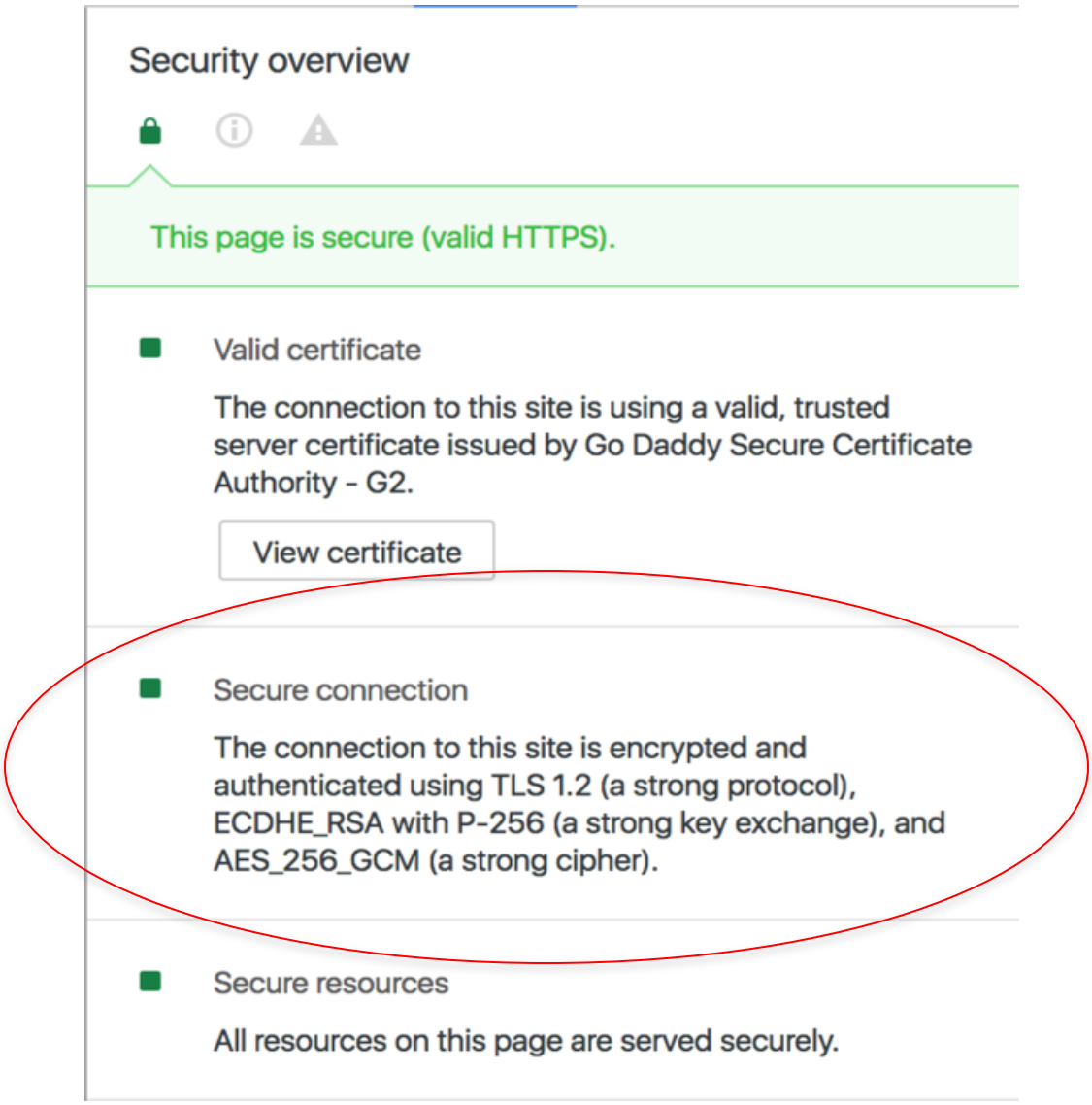


Figure 4. Transmission Encryption

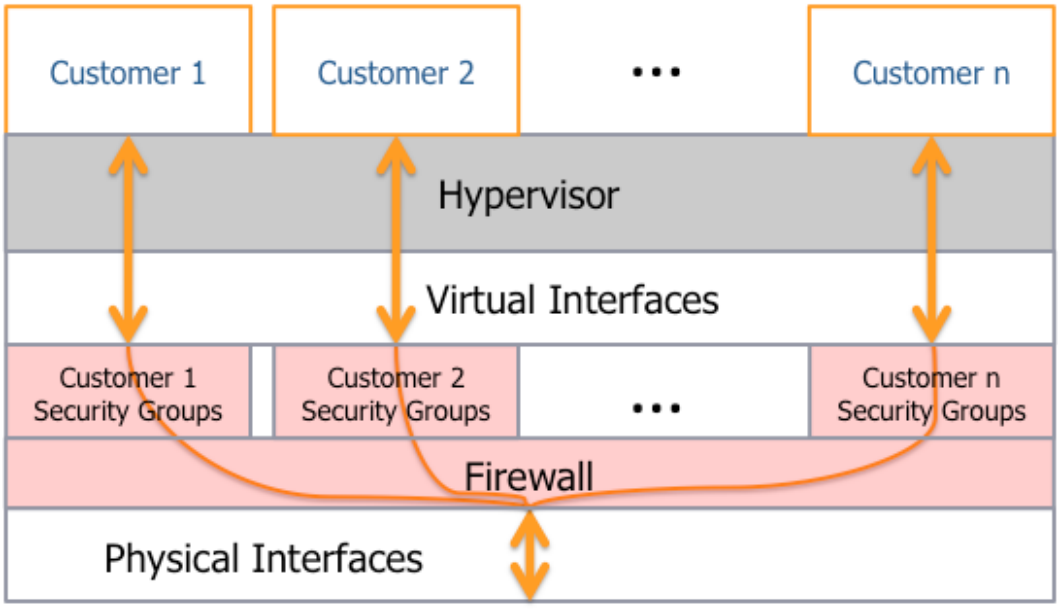
System Administration

Administrators with a business need to access the servers are required to use multi-factor authentication to gain access to host servers. These servers are systems that are specifically designed, built, configured and hardened to protect our clients' separation of data. All such access is logged and audited. When an employee no longer has a business need to access the servers, the privileges and access to these hosts and relevant systems are revoked.

Cloud Security

We use Amazon Web Service (AWS) as our cloud computing service. AWS works with Medidata's traditional data center for some of our processing. To assure that our customer data is secure in AWS we have conducted a comprehensive assessment of the AWS security.

- Physical Security: Military grade with multiple layers of manual and automated controls
- Logical Security: Stellar
    1) AWS is subjected to reviews by a large number of clients, including U.S. Department of Health and Human Services (HHS)
    2) AWS is monitored 24x7 by a dedicated security team
    3) With a plethora of clients, they must implement security to the highest bar to cover all
    4) Medidata supplements AWS security with 24x7 SIEM monitoring of our clients and encryption
- Virtualization Security: Industry Best Practice
    1) While data is being processed, different instances running on the same physical machine are isolated from each other via the Xen hypervisor.
    2) The AWS firewall resides within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host on the Internet and can be treated as if they are on separate physical hosts.
    3) The physical RAM is separated using similar mechanisms.
    4) DDoS protection
    5) MITM (Man in the Middle) attack protection
    6) IP Spoofing prohibited at host OS level
    7) Packet Sniffing Promiscuous mode is ineffective at hypervisor level
    8) Configuration Management employed for changes



Used with AWS permission

Figure 5. AWS Virtualization

Storage Device Decommissioning

When a hard drive reaches the end of its useful life, Medidata procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Medidata uses the industry standard techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. Until a device can be decommissioned using these procedures, the device is physically stored in a locked secure environment in the server room.

Configuration Management

Emergency, non-routine and other configuration changes to existing Medidata infrastructure are authorized, logged, tested, approved and documented in accordance with industry norms for similar systems. Medidata communicates with our customers prior to an urgent "out of cycle" software update or infrastructure repair to minimize any impact on the customer and their use of the services. Medidata applies a systematic approach to managing change so that changes to customer services are thoroughly reviewed, tested, approved and well communicated.

Security Incident Response

Information Security alerts are escalated from our Security Operations Center (SOC) or Global Network Operations Center (GNOC) System to the Information Security Staff and then to the Vice President, R&D (InfoSec) and senior management. Our incident response policy details the circumstances that would trigger a customer alert and how our customers are to be informed. The policy also references the response for controlling the lifecycle of a security incident. The plan describes the stages and actions associated with those stages, from identification, preparation and containment to restoration, notification and post-mortem of an event and or incident. Under reasonable timeframe following a detection, Medidata will confirm and perform impact analysis of the security incident and inform Medidata clients through communication channels established in the Services Agreement. All issues are tracked in an online,

database-driven issue management system. Senior level management ensures information security is part of Medidata's culture.

Vulnerability Identification and Remediation

In general, security issues that have a high threat of exploitation, in combination with a vulnerability type rated critical by our internal Nessus scanning tool or authoritative external sources, will be addressed with countermeasures within 30 days. Permanent fixes will usually be implemented within 90 days. However, no patches are applied until we coordinate with our network of partners to ensure full testing and agreement. Recent worldwide issues like Heartbleed and Shellshock are examples of a high threat and critical vulnerability that were remediated within hours.

Database Security

Client information in our Rave Database is segregated using virtualization. Each client is virtualized and runs on a separate database. The other elements of our platform execute within the Amazon Web Service in a multitenancy

Figure 6 Virtual Databases

environment where multiple customers share the same application, running on the same operating system, on the same hardware, with the same data-storage mechanism. The distinction between customers is achieved during our application design, thus customers do not share or see each other's data.

Business Continuity and Disaster Recovery

Business Continuity (BCP) and Disaster Recovery (DRP)

Security Incident Response Business Continuity and Disaster Recovery Planning are viewed as a dual approach for the entire business. As such, the activities involve business management from all functional and business areas, including administrative, human resources, IT support functions, and DRP for customer products. The BCP Team is responsible for overseeing the development of the internal business program, while our Service Delivery department oversees the client disaster recovery planning. Both departments ensure that senior management invests sufficient resources into planning, monitoring and maintaining the plans.

Medidata's Disaster Recovery/Business Continuity Plan defines plans, procedures and guidelines for the company in the event of disaster. Specifically, the plan establishes procedures for recovering business operations, internal data, systems and critical internal functions to maintain Medidata in the face of unexpected events.

The plan has the following primary objectives:

- To identify, assess, and prioritize Medidata vulnerabilities to emergencies or disasters and the resources available to prevent or mitigate, respond to, and recover from them.
- To outline short-, medium- and long-range measures to improve Medidata's capability to respond to and recover from an emergency.
- To provide for the efficient utilization of all available resources during an emergency.
- To ensure the continuity of operations of Medidata in times of emergency or disaster situations.

Medidata performs traditional backup as well as site-to-site electronic replication of data to protect client data in the event of a disaster. There is a dedicated disaster recovery site distant from the production data centers. BCP/DR testing is performed annually.

Plan Components

The Plan is comprised of a number of elements; all working in concert to assure that Medidata meets all known industry and regulatory requirements.

Business Continuity Plan (BCP)

- Crisis management
- Business center relocation
- Alternate workplace options
- Comprehensive contracts with service providers

Pandemic Response Plan (PRP)

- Education
- Preventative actions to contain pandemic
- Responsibility, Governance

- Policies & Procedures

Disaster Recovery (DR)

- Annual exercises
- Documented recovery procedures
- Comprehensive contracts with service providers

Disaster Recovery (DR)

Medidata has a disaster recovery plan in place, which covers: alert lists, team responsibilities, recovery and notification procedures, resumption plans, installation tasks, work area checklists and preparedness procedures. Medidata's support, product and account management teams would notify all customers of unscheduled downtime via email initially, via phone if the situation escalates. In conjunction with the senior management team, the service delivery team designs and maintains the plan.

In the event of a disaster limited to the data center, work would continue at one of the Medidata disaster recovery sites. All production, DR and testing facilities are fully supported on redundant power feeds and Uninterruptible Power Supplies (UPS). These will provide full power until diesel generators are brought online (typically within 12 seconds).

Patient Cloud Security

As medical devices become more interconnected and interoperable, they can improve the care patients receive and create efficiencies in the clinical trial system. While designing our systems, Medidata carefully considers possible cyber security risks that might connect to medical devices, and we develop plans to manage system controls or software updates. Our guidance in this area originates in NIST SP 800-53 and NIST 800-82. These same NIST publications were the basis of the FDA recommendations.

The approach to securing the Patient Cloud software differs from the rest of the Clinical Cloud software since part of it is its executing on a mobile device. The Medidata security team has taken the following steps to assure Patient Cloud's safety:

- Reviewed the design of the application and ensured that all communication to/from the device is encrypted. Due to the strength of the encryption we obtained an evaluation and approval from the US Government to export the encryption built into our software.
- Medidata performs a penetration tests by a number of third parties, including Optiv, BlackHills InfoSec & Coalfire Labs, to identify any security weaknesses.
- The operational architecture was reviewed during several design meetings to make sure all information was being protected from device to storage in our data centers. The data center security for all of our products is covered in this white paper.

Protected Health Information

The following information about electronic protected health information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is provided for informational purposes to Medidata Imaging Customers, and is not legal advice.

PHI is defined as a set of eighteen identifiers that, if present, allow for the identification of a specific individual's health information. Pursuant to HIPAA and related regulations, PHI must be protected under certain circumstances, including the requirement for entities handling PHI to execute Business Associate Agreements ("BAAs").

Regarding Medidata Imaging, HIPAA is not applicable where:

1. PHI is not collected (does not reach Medidata Imaging servers);
2. PHI is collected under a patient authorization (e.g., as part of the Informed Consent in a clinical trial); or
3. PHI is collected for purposes of patient treatment (the patient treatment exception)

In further detail regarding whether PHI is collected (#1 above), Medidata Imaging's offerings may be configured to avoid the collection of PHI in the first instance. The offerings provide an "applet" for installation on customer systems; the applet can then be configured to perform PHI redaction (e.g., of DICOM header information) prior to the secure transfer of any data to Medidata Imaging. The result is that the data is no longer PHI when it is securely transferred out of the customer's systems to Medidata Imaging's servers.

In addition, certain image types do not contain PHI, regardless of their DICOM header information; such images would not be subject to HIPAA requirements.

Healthcare sites and other entities who contract with sponsors or contract research organization (CROS) (an Medidata Imaging Customer") should direct any further questions regarding Medidata Imaging security or privacy controls to the Medidata Imaging Customer.

Medidata Regulated Content Management (RCM)

Medidata acquired CHITA, now known as Medidata RCM, in February 2017. RCM provides users with the ability to create, store, view, edit and jointly work on both regulated and non-regulated content in a single application. The security control strategy for RCM is based on ISO 27001:2013 and as such the policies and procedures outlined in this White Paper also apply to Medidata's management of RCM.

Medidata RCM currently processes in two Equinix co-location data centers, one in San Jose, CA and the other is Ashburn, VA. Infrastructure support services at these data centers are provided by Synoptek. Equinix data centers have annual Service Organization Control (SOC-1 and SOC-2) audits and are ISO 27001 certified.

Frequently Asked Questions

1. *Is the Amazon Web Service as safe and secure as a traditional data center?*

Security in the cloud is similar to security in Medidata's organic data centers. From the client perspective there are no physical servers or storage devices; both use software-based security tools to monitor and protect the flow of information into and out of the computing resource.

How is it the same?

- The security tools and techniques Medidata uses in our data center are used in the cloud.
- The same operating system (OS) and Medidata applications are used and updated with the latest security patches, backups of your data, anti-virus, intrusion detection and security incident and event monitoring (SIEM) tools.
- Medidata sets up subnets to separate environments that should remain isolated from one another—for example, we separate our development and test environment from your production environment—and then configures network Access Control Lists (ACLs) to control how traffic is routed between them.
- We have multiple users—like developers, testers and administrators—and provide them with their own unique credentials for accessing AWS resources. We even require them to use multifactor authentication.
- We use network monitoring and security management tools from SumoLogic to collect and analyze logs and network traffic information from our resources; this allows us to respond to events realtime notifying customers within 24 hours of any substantial risk to their environment.
- Medidata performs vulnerability scanning on our systems.
- We are also on the verge of establishing a Virtual Private Cloud (VPC) from our data center to our cloud resources to add an additional layer of transmission protection. In the VPC our clients will be operating in a private subnet, not the traditional public subnet.

How is it different?

- Our administrators/developers manage AWS resources remotely instead of locally.
- We use software-based security mechanisms instead of hardware-based solutions.
- Instead of racking and stacking, our IT support folks will be launching and configuring.
- Authentication using digital signatures and crypto keys is required for every Medidata application running in AWS.
- Instead of just a firewall protecting all of your resources, every virtual server also contains a security groups that act like a secondary firewall. Additionally, TrendMicro has local firewalls configured on each server.
- The software is hardened through a baseline image of our virtual server (EC2 instance). We create an Amazon Machine Image (AMI), which is a template that includes our OS, libraries, applications, configurations, etc. We can then save that baseline image and have it automatically loaded on every new instance launched.
- Operating in a SaaS model versus an onsite data center is physically different. But AWS data centers must meet Medidata's specific security requirements and possess certifications like SOC2, ISO 27001 and Safe Harbor.

Security Advantages of the Cloud

- **Instant visibility into our inventory**
  The first step in securing assets is to know what they are. With tools like AWS Config and resource tagging, we can always see exactly what cloud assets we're using at any moment.

- **Additional security tools**
  AWS provides Medidata with a list of security tools specifically designed to monitor and configure the AWS virtual space that we use.

- **Significant DDoS protection**
  AWS's size and scale makes them more capable and DDoS resilient. The AWS infrastructure is equipped to handle extremely large amounts of traffic; and when we use AWS services like ELB, Auto Scaling, CloudWatch and CloudFront, Medidata can architect a highly available system that can help weather DDoS attacks.

- **Security economies of scale**
  Medidata and its customers reap the same security benefits as the largest corporations when we're in the AWS cloud. In addition to Medidata's dedicated security team, AWS also has a large, dedicated security team and a variety of systems and tools that continuously monitor and protect the underlying cloud infrastructure.

- **Continuous hardware replacement and upgrade**
  AWS is always improving their infrastructure. They replace end-of-life hardware with the latest processors that not only improve performance and speed, but also include the latest secure platform technology, like the Intel AES-NI encryption instruction set, which significantly speeds up the execution of the AES algorithm that Medidata uses.

2. *Why does Medidata use FTPS instead of SFTP?*

The two industry standard protocols available for Secure FTP transfers are SFTP (FTP over SSH) and FTPS (FTP over SSL). Both SFTP and FTPS offer a high level of protection since they implement strong algorithms such as AES and Triple DES to encrypt any data transferred. Both options also support a wide variety of functionality with a broad command set for transferring and working with files. So, the most notable differences between SFTP and FTPS is how connections are authenticated and managed.

With SFTP a connection can be authenticated using just a user ID and password to connect to the SFTP server. SSH keys can also be used to authenticate SFTP connections in addition to, or instead of, passwords. With key-based authentication, a user would need to generate a SSH private key and public key beforehand. When you connect to the SFTP server, your software would transmit your public key to the server for authentication. If the keys match, along with any user/password supplied, then the authentication will succeed.

With FTPS a connection is authenticated using a user ID, password and certificate(s). Like SFTP, the users and passwords for FTPS connections will also be encrypted. When connecting, your FTPS client will first check if the server's certificate is trusted. The certificate is considered trusted if either the certificate was signed off by a known certificate authority (CA), like VeriSign, or if the certificate was self-signed (by your partner) and you have a copy of their public certificate in your trusted key store.

In summary, SFTP and FTPS are both very secure with strong authentication options. However, since FTPS is much safer to port through our firewall, it fits our overall security architecture, and we are seeing an increasing percentage of clients adopting FTPS, FTPS was the clear winner for our secure FTP needs.

3. *What third-party products are used for processing?*

Product: **Google Analytics**
Category: Site Usage Tooling
Medidata Use: Tracking website usage. It provides information on user location, language they are requesting, some performance information, what is done on our site, length of connection, etc. Google Analytics encrypts its data at rest and stores this data in its own secure data centers.

Product: **SocketLabs**
Category: Email as a service
Medidata Use: User data that we send to SocketLabs includes: a) study and study group names; b) the contents of the custom email property of a study and study group. This is user configurable but it is typically just instructions on signing up and more information about the pharmaceutical company and the study; c) email addresses of all of our users; (d) the names of users who are administrators; (e) activation codes for all user accounts. All the data that we send to SocketLabs is also put into emails, so it is data that can be handled by servers anywhere in the world, no matter which email provider is used. Innocuous data includes: the Medidata logo, and boilerplate language about being invited to a study and changing your email address.

Product: **NewRelic**
Category: Application performance management
Medidata Use: Medidata uses NewRelic to gather performance metrics on our deployed applications, both in production and non-production environments. These metrics include transaction response time, web traffic throughput and Apdex score. These metrics are broken down by deployed instance and are available both for live traffic and historical data. We also capture slow transactions with NewRelic and detailed information on these slow transactions stored in the NewRelic system, including a comprehensive list of the calls (both web service and database) made during the slow request. In order to collect these data from our servers, we install NewRelic collector daemons on our servers. NewRelic hosts our data in its own secure data centers. Also, data sent to NewRelic in secured in flight with TLS.

Product: **SumoLogic**
Category: Log aggregation and analytics
Medidata Use: Most of Medidata's suite of applications send their application, web server and app server logs to SumoLogic on a periodic basis (generally new log lines are sent to SumoLogic every few seconds). We employ SumoLogic's collectors on our servers to buffer and send logs to SumoLogic. We ensure that sensitive information, such as user passwords, third-party credentials, is not written to our logs, either on server or in SumoLogic. SumoLogic sends our historical log files to AWS's Simple Storage Service (s3) on our behalf so we can undertake analysis of this historical data with, e.g., map-reduce tools if need be. SumoLogic also has a UI and API for log analysis, alerting and custom dashboarding.