MEDIDATA | WHITE PAPER

Security Whitepaper

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

Table of Contents

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

Table of Contents Continued

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

Executive Summary

Medidata recognizes that an effective information security and cyber defense program must address the entire product lifecycle, including the design, development, production, distribution, deployment, maintenance, and disposal of a product and any of its associated data.

Medidata has implemented administrative, technical, and physical safeguards to help protect against security incidents and privacy breaches involving all Medidata products, provided those products are used in accordance with Medidata instructions for use. However, as systems and threats evolve, no system can be protected against all threats and vulnerabilities. Forward looking strategies and continual assessments are key components of a sound program for defense. Our customers are important and we partner with you to maintain security and privacy safeguards for all of our managed data and services.

If you have any concerns, we ask that you bring them to our attention, and we will investigate. Where appropriate, we will address the issue with product changes, technical bulletins, and/or responsible disclosures to customers and regulators. Medidata continuously strives to improve security and privacy throughout the product lifecycle using practices such as: privacy and security by design, product and supplier risk assessment, vulnerability and patch management, automated vulnerability scanning, external third-party testing, access controls appropriate to customer access and data, and incident response.

"Information Security is crucial to the protection of patient privacy and in some cases their very life; when I became a clinical trial patient, the protection of my healthcare data became personal. I can tell you that as a trial patient and security professional who understands cyber threats, Medidata is the only firm I want storing and processing my information."

- Glenn Watt, Medidata, Chief Information Security Officer (2007-2018)

Medidata is committed to our customers and encourages this audience to contact us with questions, concerns, and improvements to our products and services.

For any questions or clarifications, feel free to reach out to Medidata.asksecurity@3ds.com

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

Purpose

The purpose of this document is to discuss the publicly available information on how Medidata security and privacy practices have been applied to the Medidata Clinical Cloud (MCC). It contains narratives describing how Medidata maintains each area of security for our products, and how we can partner with you to ensure security throughout the products lifecycle.

We want to provide you with a general discussion of Medidata security issues and answers while not divulging confidential or proprietary security product names, configurations, and operating procedures. No portion of this document should be considered to meet contractual obligations as these practices and technologies may be updated without notice and updates to the document.

For more detailed, confidential queries, please refer to your Medidata point of contact/sales engineer/professional services/ account executive for information.

Medidata Security Culture

Our set of values, shared by everyone in the organization, determines how people think about and approach security. Having a robust security culture develops a security conscious workforce and promotes the desired security behaviors needed from employees. This is referred to as the "Human Firewall." Employees, both Medidata and Partners, 'know' what is out of the ordinary and suspect. Personal experience and observations cannot be automated. That is the limit of the tools we purchase and deploy.

Medidata develops its products with a "Security by Design" mindset. The OWASP software development principles establish a core strategy for our Software Development Life Cycle (SDLC) as well as the design and modification to enterprise technology architectures.

The OWASP Security Design Principles are:

- Minimize attack surface area - Reduce the functions available to a user to only what they need
- Establish secure defaults - Strong security rules managing users and their access
- The principle of Least Privilege - Users should have the minimum set of privileges required to perform a specific task
- Defense-in-Depth - Products must have multiple layers of validation, additional security auditing tools and logging
- Fail securely - Malfunctioning programs should default to less or no access
- Don't trust services - Third-Party software and services utilized within a program should not be given higher level rights and the data streams must be validated
- Separation of duties - Prevent individuals from acting fraudulently
- Avoid security by obscurity - Use sufficient security controls to keep your application safe without hiding core functionality or source code
- Keep security simple - Reduce complexity where possible to keep code visible
- Fix security issues correctly - Root cause analysis must be performed for flaws and then acted upon

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

Information Security is also a part of Medidata's business culture. Medidata's strategy for establishing Information Security Governance includes maintaining the Confidentiality, Integrity, and Availability of our customer's data, minimizing the potential for business damage from malicious events such as ransomware or a data breach.

Medidata's Governance Strategy is implemented using a combination of industry leading training and education, coupled, and supported by a diverse team of highly experienced and certified security professionals, organized around specialized capabilities including security operations, security engineering, security architecture, Incidence response, identity and access management, risk management and security frameworks. Medidata's implementation of security governance is tested and audited on an at least annual basis to ensure Medidata maintains compliance with all appropriate security and privacy requirements.

Enterprise Risk Management

Medidata's Senior Leadership Team recognizes that their responsibility to customers requires a strong control structure. Accordingly, a commitment to help ensure that effective security controls are in place has been an integral part of Medidata's overall risk management strategy. Overseen by the CISO, a member of the Senior Leadership Team, this process utilizes the output of strategic oversight to build the Strategic Risk Register. This risk register incorporates a high level view of security requirements and controls as well as operationally identified threats and emerging global cybersecurity threats.

These risks and their treatments are part of our update to the Dassault Systemes Board of Directors. We continue to have the top down support as a strategic program of the organization.

Forward-thinking organizations know that risk is everybody's business. It cannot be confined to a single line of business or performed on an ad-hoc basis within operational silos. Ownership of risk must be shared across the enterprise and be deeply collaborative and transparent. Medidata knows this to be true given the current volatility of global markets and the hard-learned lessons from the past few years, all of which significantly disrupted our economic, business and social ecosystems.

In an ideal world, the real-time information required to effectively manage and mitigate such disruptions and risk—including cyber, business, operational and reputational—would flow into a company and be shared across a well-defined group of stakeholders who work together and are empowered to make quick, well-informed decisions.

Medidata aspires to this ideal state, the goal that all of us here should work toward if we are to successfully navigate our unpredictable, fast-changing world and the expanding threat landscape that has materialized as a result.

Success at Medidata is founded on building proactive, integrated security and risk management solutions that leverage the systems and processes needed to detect potential risk events, in real time, as they unfold.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

Information Security Frameworks and Audits

Medidata implements security frameworks, security controls, and security methods from several Certifications, including ISO 27001, 27002, 27701, 27017 and 27018, SOC-I & SOC-II+, Type Payment Card Industry Data Security Standard (PCI-DSS), and NIST RMF/FISMA, as well as compliance with General Data Protection Regulation (GDPR). and other local regulations. We also have a FISMA Authority to Operate for Federal customers and are part of a National Heart Lung and Blood FedRAMP Authority to Operate. External audits, performed by certified 3rd parties, are performed annually for ISO, FISMA and SOC2 and cover pertinent details regarding the Medidata people, processes, and technology that provide and support your product, software, or service.

Each certification audit provides assurances to our current and potential customers that Medidata complies with regional, national, and international laws and regulations. Each of the audits are performed using external auditors and any findings or non-compliances are tracked in the Medidata ticketing system. These tickets contain details of the root cause and are required to be regularly updated with the efforts necessary to resolve the issue. A monthly report is delivered to Information Security Leadership for review and escalations, as necessary.

Medidata employs "best in breed" hybrid solutions (organizational and technical) based on the prescriptive requirements established by these security frameworks. This holistic approach supports a comprehensive implementation of security controls and mechanisms that meet all established requirements.

Access Control

Medidata's implementation of access control is designed to ensure all accounts are managed continuously and that access for both privileged and non-privileged accounts is limited and minimized based on roles and responsibilities for the assigned user. Access management requirements are used to provide instructions for adding/removing/changing access for all accounts, to identify the control systems to ensure restricted access is enforced, and to identify the frequency of reviews of all access granted. A variety of automated tools are used on a continual basis to enforce the management of accounts including automatically disabling accounts when required and for auditing all account management activities (account creation, modification, enabling, disabling, and removal).

Pre-approved interconnections are used to ensure information flow is enforced within the system based on established service level agreements. Medidata requires at least two administrators to coordinate account handling activities with all requests being managed by a ticketing system. Accounts are reviewed by the Quality Management team quarterly. Limiting unsuccessful logon attempts and lock-out self-healing is enforced based on guidance established by CIS Benchmarks. No actions by users or devices are allowed without identification and authentication. Remote access is enforced via MFA and encryption for all connections. All account access is monitored via SIEM and gateway protection methods.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

IDENTITY PROVIDER AND SERVICES (IDP IPS)

Medidata uses an identity provider (abbreviated IdP or IDP) for Medidata system access that creates, maintains, and manages identity information for principals and also provides authentication services to relying applications within a federation or distributed network.

Provider user authentication as a service to administer access to applications, such as web applications through outsourcing the user authentication step as a trusted identity provider. Relying party application is said to be federated, that is, it consumes federated identity. An identity provider is a trusted provider that lets you use single sign-on (SSO) to access other websites. This SSO enhances usability by reducing password fatigue. It also provides better security by decreasing the potential attack surface.

Identity providers can facilitate connections between cloud computing resources and users, thus decreasing the need for users to re-authenticate when using mobile and roaming applications.

Least privilege functionality is implemented by adhering to CIS Benchmarks configuration settings and by applying a variety of host and gateway access restrictions.

IDENTIFICATION, AUTHENTICATION, AND AUTHORIZATION

Medidata implements identification and authentication methods consistent with requirements established by ISO and NIST. All users, both Medidata staff and customer users, are authenticated using unique IDs. User accounts and passwords are required to be user specific with no permitted sharing of credentials. Medidata also enforces multi-factor authentication for all staff and offers optional multi-factor authentication to our customers.

The MCC provides access and authorization controls, a comprehensive audit trail and an e-signature system to link electronic signatures to an electronic record, establishing non-repudiation. Medidata requires its customers and its personnel to sign an understanding of these requirements, both when activating user accounts and when managing and supporting operations.

CYBERSECURITY AND INFORMATION SECURITY AWARENESS TRAINING

Medidata's implementation of cybersecurity training is designed to ensure all employees including contractors receive the appropriate training for their position and security responsibility.

Several targeted training modules are used across Medidata. Annual training is tracked, and employees or contractors not completing the coursework have their access revoked from all Medidata systems. Permanent reinstatement requires completed training and manager's approval.

Training is managed through elearning training courses via Medidata's learning management system, and additional courses are also available on-demand within the 3DS learning management system.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

AUDITING OR MONITORING

Medidata's implementation of security event auditing is designed to ensure all required auditable events are captured and are consistent with the ISO 27001 family and NIST requirements. Medidata uses a variety of SIEM tools to monitor and audit against these requirements which includes auditing for security breaches, intrusion attempts, integrity events, system and component failures, and user activity events. All auditable events are monitored on a continuous basis.

SIEM

A Security information and event management (SIEM) capability is implemented across the entire environment. FIPS 140-2 compliant cryptographic methods and solutions are used throughout the system.

Configuration Management

Medidata implements configuration management throughout the lifecycle of all systems and components using a variety of configuration change management tools, processes, and procedures. Baseline configurations are maintained in validation packages supported by automated tools. All changes are tracked systematically. Test and validation are an integral part of the configuration management process. Security and privacy representatives are members of the Change Review Board (CRB) and provide security and privacy risk assessments when appropriate.

BUSINESS CONTINUITY AND DISASTER RECOVERY (BC/DR)

Medidata implements a comprehensive Business Continuity and Disaster Recovery (BC/DR) capability that is applied across the whole organization.

The planning process is driven by not only the needs of Medidata itself but also driven by the requirements of our customers as they are expressed in SLAs. All key individuals and organizations within Medidata participate in the annual exercise and review of the disaster recovery plan including our service delivery, customer success, and professional services teams. Our planning process includes recovery of all mission and business functions within the recovery time objectives established by our customer SLAs. All critical system assets as well as all mission and business functions are identified during this planning process. The resulting plan is tested no less than annually with feedback and test results used to continuously improve our capabilities.

INCIDENT RESPONSE AND HANDLING

Medidata maintains a comprehensive incident response plan that allows for the prompt identification, containment, and remediation of immediate threats to the confidentiality, integrity and availability of systems and data.

Medidata maintains a dedicated 24x7 security operations team, Global Network Operations Center (G-NOC) to monitor and provide support for all incident handling activities. Medidata's security operations team uses a variety of automated incident management tools including a SIEM and a variety of logging and event management and reporting tools. 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. Medidata integrates incident response training and testing into its annual disaster recovery testing.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

MAINTENANCE

Medidata implements a rigorous maintenance program that includes prioritization and approval requirements for all changes made with the overall objective to ensure that all security protections remain fully intact. Vulnerability scanning, application scanning, and malware protection measures are implemented to check all media used during a maintenance activity. External devices are not allowed to connect without first being scanned and then only when under the control of the operations staff. All maintenance is documented and authorized as part of a change management process and includes a roll-back plan and test and verification requirements.

MEDIA PROTECTION

Medidata implements media protection at each location where data is processed or stored. All data is treated as restricted access data with access managed by our operations staff. This includes access for the purposes of destruction, removal, backup, and restoration of data. All media designated for destruction is tracked and results in destruction certificates for each media destroyed. Media is never reused outside of Medidata. All media in use, in transit, or in storage is protected using FIPS 140-2 compliant cryptographic methods to ensure data integrity and confidentiality are maintained.

DATA LOSS PREVENTION

At Medidata, Data Loss Prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR. Once those violations are identified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Data loss prevention software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use. DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response.

ENVIRONMENTAL SECURITY

Physical access to facilities and protected information assets that are restricted to authorized personnel. Medidata maintains current lists of personnel with authorized access to facilities containing information systems and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials at least annually.

No areas are publicly accessible by design. The physical access list is maintained by the building custodian but is reviewed on a periodic basis by the facilities security team. A combination of biometrics, smartcard, and PIN code are required, in correct order, to access the data center. Additions to the access list must be approved by senior management before unescorted entry is provided.

Medidata monitors physical access to information systems to detect and respond to physical security incidents. Physical access is logged automatically and available for review. Cameras are used to record physical access.

Medidata controls physical access to information systems by authenticating visitors before authorizing access to facilities. Access by a visitor is preceded with a request for access and approved by appropriate Medidata personnel. All visitors are escorted within the facility.

Medidata maintains a formal Information Security policy with documented procedures regarding physical security of secure areas and equipment.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

SECURITY PLANNING

Medidata implements a continuous security program improvement process founded on ISO 27001. An ISO 27001 certified Information Security Management System has been implemented along with a NIST compliant System Security Plan for Medidata Clinical Cloud. These plans are updated annually to incorporate new and changing security and privacy architecture requirements and to ensure robust Medidata security capability. This approach ensures that all security and privacy architecture changes are incorporated into security plans, type 1 qualification documents, engineering documents, product documents, and hosting documents.

PERSONNEL SECURITY – HUMAN CAPITAL

Employees are hired in accordance with workforce conduct standards, considering results of background checks performed as they relate to background screening procedures. All personnel are required to read, acknowledge, and comply with the Code of Business Conduct prior to receiving access to Medidata systems. Completion of this is captured in Medidata's learning management system. These personnel security processes are also applied to third-party contractors and consultants.

PRODUCT AND SERVICE QUALIFICATION

Medidata implements a comprehensive acquisition process that is planned, documented, and approved on an annual basis and that includes consideration of security and privacy requirements. This includes funding for penetration testing, FISMA evaluations, ISO audits, SOC 2 audits, Privacy Shield certifications and other security related activities. Planning also includes funding for encryption products and software needed to incorporate new security and privacy features into system software. The information security and privacy teams are involved in the acquisition process to ensure all security and privacy requirements are included during the acquisition.

SYSTEM AND INFORMATION INTEGRITY

Medidata implements system and information integrity assurance across the organization using automated tools, ticketing systems, patch management systems, and quality assurance processes to monitor, scan, and remediate findings throughout the lifecycle of Medidata systems. Malicious code protection is monitored and managed centrally as it is applied across the enterprise. Integrity monitoring tools are employed throughout the environment to ensure the integrity of Medidata systems. Information within the Medidata systems is encrypted at rest and in transit. Also, Medidata continually monitors the National Vulnerability Database.

THIRD PARTY RISK MANAGEMENT (TPRM)

Medidata uses third parties and sub-service providers who, as part of providing services, have access to and process data on behalf of Medidata, including occasionally personal information (PII)

The Medidata Privacy Office (MPO) partners with business areas, subject matter experts, and control functions to develop contracts that include provisions outlining the required privacy commitments from third parties involved in the processing of participants' personal information. The MPO and Legal Team review and approve new third-party contracts to validate the provisions relating to privacy are included according to Medidata standards.

Global Compliance & Strategy (GCS) partners with the Medidata Privacy Office (MPO), Information Security (InfoSec) and business areas ensuring all new vendors are subjected to undergo a defined risk-based evaluation of third-party vendors who access Medidata systems and environments. Medidata performs periodic risk assessments of third-party vendors focusing priority on those who access, use and/or store participants' personal information PII), analyzes the results and if deemed necessary, develops a documented plan to assess a third party vendor deemed to be higher risk because of the risk assessment. Vendor assessments are performed in accordance with the defined Medidata Supplier Evaluation policies and procedures. Results of vendor assessments are documented.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

SUPPLIER EVALUATIONS AND AUDITS

All third party vendors proposed for use in support of the Medidata SDLC or for providing services to Medidata, Medidata clients or Medidata partners shall be subjected to security evaluations by Medidata personnel. Medidata evaluates suppliers, both initially and on an periodic basis, to ensure that basic operational security metrics are being met to Medidata's requirements. At a minimum, Suppliers are periodically evaluated. Critical Suppliers are evaluated within 12 months of last evaluation. Major Suppliers are evaluated within 12-24 months of last evaluation. Minor Suppliers are evaluated with 24-36

Supplier audits and/or questionnaires may be scheduled because of an unexpected event concerning the supplier, irrespective of the frequency of audit and/or questionnaire. Logistical supplier audit information including date of announcement, date of audit and completion date, is maintained in the supplier status/schedule.

ANTI-VIRUS AND ANTI-MALWARE PROTECTION

In addition to our Intrusion Detection System (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.

DATA ENCRYPTION

All data including PHI and PII is stored and transmitted in encrypted form using the latest Advanced Encryption Standard algorithms (AES-256) and are regularly tested for recoverability.

DATA ENCRYPTION IN TRANSIT

The system uses Transport Layer Security TLS v.1.2 to achieve encryption for data in transit. TLS v.1.2 allows client computers to establish a publicly accessible connection with servers, however only the client and server will be able to decrypt, or view in interpretable and usable form the information being transmitted.

ENCRYPTION-AT-REST

Encryption is enabled at the storage unit level and is affected through hardware. For the Rave EDC data stores, the Hitachi Storage Area Network uses 256-bit Advanced Encryption Standard (AES) keys, using a proprietary key management system. For our multi-tenant systems, we also use AES-256, but use Amazon's KMS Product.

SYSTEM HARDENING STANDARDS

Medidata implements CIS benchmarks hardening guidance on all MCC components.

REMOTE CONNECTIVITY

By default, Medidata only allows inbound traffic from port 443. The firewalls and intrusion and prevention detection systems ("IDP") blocks source and destination ports, as well as ensure traffic safety. A 24x7 Global network Operations Center ("GNOC") is in operation to help ensure someone is always monitoring the environment. Additionally, Medidata has engaged a third-party Managed Security Service Provider (MSSP) to provide 24x7 coverage of the security environment and is empowered to take action to protect the environment, with a service level agreement (SLA) of fifteen (15) minutes.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

Privacy Program

The Medidata Privacy Office ("MPO") implements the privacy principles within the Global Privacy Program based on Medidata's role in the processing of personal data on behalf of its customers. Medidata's customers act as "data controllers" with respect to the personal data that is submitted and processed within the MCC for their contracted services. Data controllers (or similar entities as defined in applicable law) refers to the entity that determines the means and purposes of the processing of personal data. That is, Medidata's customers act as their own data controllers and decide what personal data will be collected, submitted, processed, disclosed, retained, and/or destroyed when they leverage the MCC for clinical trials, and for what purposes those activities take place. Medidata's role is that of a "data processor", the entity that carries out the instructions of a data controller to implement the means and purposes of processing that have been decided upon.

Medidata as a data processor is primarily responsible for implementing effective data security measures and for following our customer's instructions with respect to the above areas of responsibility.

- Data retention and disposal policies and procedures for proper processing and secure maintenance, disposal and destruction for system hardware and sensitive data, based on applicable agreements, laws, and regulations.
- Privacy commitments to user entities are documented and communicated in customer contracts/agreements. Such privacy commitments include, but are not limited to, the following:
- The Medidata Privacy Office (MPO) maintains the Global Privacy Program to regulate the collection, access, use, storage, disclosure and disposal of customers' personal data in compliance with applicable laws and best practices
- User entities are informed of Medidata practices with respect to personal data as part of 'Terms of Use' visible when logging on to the MCC
- Medidata performs "Privacy by Design" assessments for each product release of MCC to assess the impact/any material changes to the processing of personal data
- Medidata maintains a Customer Data Governance program to validate appropriate access and use of Customer Personal data
- Medidata returns or deletes Customer Personal data upon customer request (in accordance with applicable regulatory/ legal requirements)
- The MPO maintains a Privacy Incident Response program for identifying and evaluating unauthorized disclosures of customer personal data

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

PRIVACY BY DESIGN

Medidata has formally documented application and data inventories that document the source and location of Personally Identifiable Information across the MCC. The application and data inventories are prepared by each Product Team as part of the Privacy by Design process. A standard template is documented and maintained per each business process area that specifies what kind of data is collected, associated privacy risks within that business process, and the controls in place to mitigate privacy risks identified through this process.

As part of the Privacy by Design process, Product Owners evaluate projects that result in new and/or changes to existing processes that access, use and/or store participants' personal information to assess the impact on personal information and related controls. Where such changes are identified, the MPO assesses the risks associated with any changes to how personally identifiable information is processed in the MCC. Control gaps identified as part of the Privacy by Design process are documented and corrective action plans are developed and executed to address the gaps.

Security by Design

SECURE CODING STANDARDS

Medidata incorporates secure application development in its SDLC process. It has formal coding standards and coding guidelines under version control, as they are stored within our source code repository.

SOFTWARE DEVELOPMENT LIFE CYCLE

The MCC provides end-to-end technology and data analytics solutions designed to manage activities across the clinical development process. As a SaaS environment, the Medidata platform is scalable and expandable, per customers' requirements. Medidata accomplishes this through adherence to a documented SDLC process driven by Agile development principles, building in quality throughout the process. Medidata produces software that resides on qualified infrastructure, meets customer requirements, functions as purported, and supports compliance with applicable GCP, Data Protection/ Data Privacy, and Electronic Records/Electronic Signatures ("ERES") regulations and guidance. The SDLC requirements and process are documented within SOP-SDLC-013 Develop and Release Software Product. The IT infrastructure qualification requirements and process are documented within SOP-ITH-013 Hosting Environment Architecture Management.

SDLC activities are undertaken by the One R&D department. Functional departments exist within One R&D, each with management responsibility and authority for the design, development, testing, validation, deployment, and operational support of Medidata software. Type of software releases include alpha releases, beta releases, feature releases, standard software releases, and urgent software releases.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

VULNERABILITY IDENTIFICATION AND MANAGEMENT

A Medidata vulnerability assessment is a systematic review of potential security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

APPLICATION SECURITY VULNERABILITY ASSESSMENTS

Medidata's primary goal in conducting security vulnerability assessments of the software Medidata produces for our clients is to identify vulnerabilities in system, network, and application security controls that could be exploited to gain access to the systems and designated data that an unauthorized user should not be able to obtain. Assessments are to include dynamic (DAST) and static (SAST) code analysis security scans. Working within the defined parameters of the test, Medidata will attempt to identify and exploit whatever system, network, and application vulnerabilities are identified to achieve the above stated goals.

No attempts will be made to disguise any attacks, as these are not stealth security assessments. It should be noted that real attacks might not be as obvious to system administrators. The testing process may be manual to limit generic results from scanners and checklist methods used in general vulnerability assessment. Alternatively, automated tools may also be used for application-mapping and potential vulnerability identification. In this way the tester can focus on directed logic based testing against applications.

NETWORK SECURITY VULNERABILITY ASSESSMENTS (PEN TESTS)

Medidata's network vulnerability assessments will include resources such as servers, switches, routers, and workstations that can be reached from a test location outside the Medidata network. Medidata will perform testing of the networks and components using carefully scripted testing methodologies approved by the Chief Information Security Officer (CISO). The Rules of Engagement specify that any testing performed will not include the testing of interconnecting network components not owned and/or operated by Medidata. Additionally, testing is not to include activities that intentionally result in a Denial of Service (DoS) to any systems or intentionally damage any exploitable target system encountered. External vulnerability assessments will be performed from location(s) outside of the physical Medidata locations/networks.

Independent Testing and Review

Security is only as good as an objective observer says it is. So, in addition to our customer and regulator assessments, we use multiple independent entities which we regularly rotate, to prevent complacency and ensure we bring objectivity, cutting edge techniques and emergent technologies to bear in order to ensure that the intellectual property of our customers and their patients are properly protected.

SOC-II is a voluntary compliance standard for service organizations, developed by the American Institute of CPAs (AICPA), which specifies how organizations should manage customer data. The standard is based on the following Trust Services Criteria: security, availability, processing integrity, confidentiality, privacy. A SOC-II report is tailored to the unique needs of each organization. Depending on its specific business practices, each organization can design controls that follow one or more principles of trust. These internal reports provide organizations and their regulators, business partners, and suppliers, with important information about how the organization manages its data.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

There are two types of SOC-II reports: Type 1 describes the organization's systems and whether the system design complies with the relevant trust principles. Type 2 details the operational efficiency of these systems.

Medidata maintains a SOC-II+ Type 2 to demonstrate Medidata's commitment to security relevant to security 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) and the additional criteria determined by Medidata Solutions, Inc. related to development and deployment, quality assurance, and electronic records and signatures

The SOC evaluation is conducted every 6-Months on a sliding 12-Month population timebox. Medidata also maintains a SOC-I Type 1 for the MCC CTMS Site Payment offering.

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 by our trained and certified Internal Security Assessor. We also apply it to any financial processing related information that is used as part of our MCC CTMS Site Payments offering.

ISO/IEC 27001

ISO 27001 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/IEC 27001 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/IEC 27001 certification standard.

The ISO/IEC 27001 certification is paired with the ISO/IEC 27701 covering the requirements for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS).

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

ISO/IEC 27017

ISO/IEC 27701 is an information security code of practice for cloud services. It's an extension to ISO/IEC 27001 and ISO/IEC 27002, and it provides additional security controls for cloud service providers and for cloud service customers.

ISO/IEC 27018

ISO/IEC 27018 is a security management standard that specifies security management best practices and comprehensive security controls in the context of Privacy Information in a cloud computing environment. This standard complements ISO/IEC 27001 and other security frameworks in order to maintain effective management of privacy related information.

Like ISO/IEC 27001, ISO/IEC 27017, and 27018 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 certification standard.

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 NIST (National Institute of Standards and Technology Special Publication) SP 800-53, Revision 5. 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 and has been awarded an Authority to Operate (ATO) by a number of US Government agencies.

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.
  - o (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.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company

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 endpoints and terminating load balancers in Medidata 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.

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.

Closing

We feel that the Medidata security practice is world-class, composed of the best people, processes and technology. We take our responsibilities seriously and earn our customers and their patients trust each and every day. We are proud of what we do and are happy to show it.

In addition to this document, we post vulnerability summaries, penetration tests results, certifications, audits and other security related matters at https://www.medidata.com/en/trust-and-transparency so that our customers and their sites can have a level of comfort in that the protections are what the patient expects.

For any questions or clarifications, feel free to reach out to the Medidata Information Security Frameworks Team at Medidata. asksecurity@3ds.com

Disclaimer

The information contained in this Security White Paper is for reference purposes only.

Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify, or supersede the terms and conditions of any written agreement between such customer and Medidata, or Medidata subsidiaries or affiliates (collectively, “Medidata”).

Medidata does not make any promises or guarantees to customers that any of the methods or suggestions described in this Security White Paper will restore customer’s systems, resolve any issues related to any malicious code or achieve any other stated or intended results. The Customer exclusively assumes all risks of utilizing or not utilizing any guidance described in this Security White Paper.

Copyright 2022 Medidata Solutions, Inc., a Dassault Systèmes company