MediCompli
SOLUTION

SECURITY PROTOCOLS FOR MEDICOMPLI

THE SOLUTION FOR THE MEDICAL DEVICES INDUSTRY

CONTENTS

USER NOTICE

Customers are responsible for making their own assessment of the information outlined in this document.

THIS DOCUMENT:
(a) is for informational purposes only, (b) represents current MediCompli product offerings and practices that are subject to change without notice, and (c) does not create any commitments or assurances from MediCompli and/or its affiliates, suppliers or licensors. The responsibilities and liabilities of MediCompli to its customers are controlled by MediCompli agreements which this document is not part of, nor does it modify any agreement between MediCompli and its customers.
This document is intended to answer questions, such as how MediCompli keeps customer data secure, and more specifically, describes MediCompli's physical and operational security processes for the Server infrastructure under the management of MediCompli on Amazon Web Services (AWS).

INTRODUCTION

Traditionally, organisations looked to the cloud for cost savings, but now, factors such as security are becoming more of a motivator.

As a cloud-first pioneer, MediCompli is well-equipped in understanding the security implications of the cloud model, with hosting services designed to deliver better security than most traditional on-premise solutions.
Security is our top priority and we run on the same infrastructure that we make available to our customers. It's central to our everyday operations in terms of how we address threats and is prioritised in the same way we handle customer data. It's the cornerstone of our account controls, and compliance audits as part of the ISO 27001 certification.
This white paper outlines our approach to security and compliance for our hosted cloud solution, MediCompli, and the software applications we handle with a transparent overview of how customer data is protected.

SHARED RESPONSIBILITY MODEL

Before covering the details of how MediCompli resources are secured, it is important to understand how security in the cloud differs from security in on-premise data centers.

When you move computer systems and data to the cloud, security responsibilities become shared between you, MediCompli and your cloud service provider (AWS). In this case, AWS and MediCompli are responsible for securing the underlying infrastructure that supports cloud, while you, the customer, are responsible for anything that's added or connected to the cloud. This shared security responsibility model can reduce your operational burden in many ways, and in some cases even improve your default security posture without additional action on your part.

AWS	HARDWARE/AWS GLOBAL INFRASTRUCTURE			
	Regions	Availability Zones	Edge Locations	
	SOFTWARE AND SERVICES			
	Compute	Storage	Database	Networking

MediCompli	PLATFORM AND APPLICATIONS			
	Operating System	Security Patching	Vulnerability Management	Application Installation Database Administration
	NETWORK			
	Security Groups / Firewall	Subnets	VPC	Network ACL Intrusion Detection And Prevention
	DATA AND BACKUP			
	Snapshot Backups	Data Volumes	Encryption at Rest	Data Transfer

Customer	POLICY AND COMPLIANCE
	Ensuring that the system meets your business needs and is operated in accordance with industry, regulatory and legislative compliance obligations.
	USERS
	The creation and management of user accounts.
	INFORMATION
	The content stored within MediCompli applications.
	MARKETPLACE APPS/PLUGINS
	Third-party services that require access to your information including how they integrate with MediCompli products.

AWS SECURITY RESPONSIBILITIES

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is the number one priority of AWS. And while you can't visit their data centers or offices to see this first-hand, they provide several reports from third-party auditors who have verified their compliance with a variety of computer security standards and regulations.

MEDICOMPLI SECURITY RESPONSIBILITIES

With the AWS Cloud, MediCompli provisions virtual Servers, storage, databases, and networks. AWS products that fall into the well-understood category of Infrastructure-as-a-Service (IaaS), such as Amazon EC2, and Amazon VPC, are under MediCompli's control, for which all of the necessary security configuration and management tasks are performed. As an example, for EC2 instances, MediCompli is responsible for managing the guest OS (including updates and security patches), any application software or utilities installed on the instances, and the configuration of the AWS provided firewall (called a security group) on each instance. AWS managed services like Amazon RDS, provide all of the resources MediCompli needs to perform a specific task — but without the configuration work that comes with it. With managed services, you don't have to worry about launching and maintaining instances, patching the guest OS or database, or replicating databases — AWS handles it.

CUSTOMER SECURITY RESPONSIBILITIES

As the customer, you are responsible for managing the information and data within your accounts, the users and user accounts accessing your data. You also control which Marketplace apps (formerly add-ons) you install and trust. When using our applications, you are responsible for ensuring your business meets compliance obligations.

RESPONSIBILITIES INCLUDE:

- Policy and compliance: Ensuring that the system meets your business needs and is operated in accordance with industry, regulatory and legislative compliance obligations.
- Users: The creation and management of user accounts.
- Information: The content stored within MediCompli applications.
- Marketplace apps: Third-party services that have access to your information, and their ability to integrate with MediCompli products.

SECURITY AS A CULTURE

At MediCompli, we have an active and comprehensive security culture which is introduced to employees at the onboarding stage.

Our Information Security Management System (ISMS) is ISO 27001 certified — the leading international standard to have for Information Security Management Systems. The accreditation provides a holistic approach to information security by assessing the risk of people, processes and IT systems.

We obtained the standard in October 2019, because it enabled us to further protect the confidentiality of our assets, and maintain the integrity of data and the availability of IT systems, thus reducing the risk of disruptions.

In addition, we hold a Cyber Essentials certification which is a government-backed scheme built to protect organisations against the threat of cyber attacks.

Our customers are confident in our ability to protect their data as a result of our efforts to obtain high-level security standards.

Crucial knowledge is not limited to key stakeholders, and employees are required to undergo training to ensure they adhere to the requirements of security best practices. Refresher training is compulsory and must be completed on an annual basis. Staff are also encouraged to refer to the documentation available on Confluence — our collaboration wiki tool. On Confluence, employees can access policies and procedures that outline business continuity plans, risk management, and so on.

Such certifications take a lot of hard work to obtain, but we felt it necessary in building and maintaining the trust and confidence of our customers. We want businesses to know how seriously we take the protection of their information, especially at a time when digital threats are rife.

Our practices expand into our services and partnerships which are outlined in the relevant sections of this document.

EMPLOYEE BACKGROUND CHECKS

Before an employee joins our organisation, their education and previous employment is checked along with the internal and external references they provide. The extent of these background checks is dependent on the desired position. Our HR team ensures all candidates, regardless of permanent, temporary or contract, are screened appropriately.

SECURITY TRAINING

All MediCompli employees undergo security training as part of the onboarding process and receive ongoing training throughout their careers (refreshed annually). Depending on their job role, additional training on specific aspects of security may be required. For instance, the IT team instructs new engineers on topics including technical vulnerability management.

INTERNAL AUDIT AND COMPLIANCE ROLES

MediCompli has a dedicated third party that reviews compliance with security laws and regulations around the world. As new auditing standards are created, controls, processes, and systems are determined. MediCompli facilitates and supports independent audits and assessments from third parties when required.

OPERATIONAL SECURITY

Far from being an afterthought or the focus of occasional initiatives, security is an integral part of our operations.

VULNERABILITY MANAGEMENT
Vulnerability management practices are in place to proactively prevent exploitation and potential losses of sensitive data. MediCompli may create and document systematic and accountable practices to maintain control programs and applications to evaluate installed and new devices and systems for vulnerabilities and to mitigate other technical and non-technical threats. The goal of this effort is to provide an extra level of protection for MediCompli's IT resources and to ensure the compliance of best practices to reduce the impact of threats to MediCompli and its customers.

INTRUSION DETECTION AND PREVENTION
MediCompli utilises GuardDuty across its AWS estate. Amazon GuardDuty is a threat detection service that continuously monitors malicious activity and unauthorised behaviour to protect AWS accounts and workloads, including Servers. With GuardDuty, MediCompli has an intelligent option for continuous threat detection in the AWS Cloud. The service uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritise potential threats. GuardDuty analyses tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs.

The IT Operations team receives automated tickets logged for medium/high risk alerts from GuardDuty.

ATLASSIAN APPLICATION VULNERABILITIES AND SECURITY ADVISORIES

Logging and Tracking Security Advisories
MediCompli tracks all critical-severity security vulnerabilities, by monitoring the issue trackers for the relevant products on *jira.atlassian.com*. For example, *jira.atlassian.com/browse/JRA* for Jira and *jira.atlassian.com/browse/CONF* for Confluence. Security issues in trackers are marked with a security label. All security issues are listed in the notes of the release where they have been fixed.

With MediCompli being listed as an Atlassian Partner, we receive security alerts which are tracked via the Partner Portal before public release. This ensures the correct mitigation and patching methods are in place before public distribution. MediCompli internally tracks, communicates, patches, and mitigates critical security vulnerabilities via Jira Service Management.

MONITORING AND CAPACITY MANAGEMENT
MediCompli hosted systems have a tool that proactively monitors all hosted systems, including; network bandwidth, Server memory, CPU and disk space utilisation.

Actions for each type of alert are defined in an internal alert management process. For high alerts, tickets are logged via the internal Service Desk and actioned from there. Any alerts of concern are discussed in weekly meetings.

Any changes to the MediCompli network or Servers follow the IT Change Management Process.

Any instances where capacity has breached the pre-defined limits are highlighted and documented in the meeting minutes.

INCIDENT MANAGEMENT
We have a rigorous incident management process for security events that may affect the confidentiality, integrity, and availability of systems or data. If an incident occurs, the security team logs and prioritises it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. MediCompli's security incident management policies are aligned with ISO 27001 best practices.

MEDICOMPLI SOLUTION

MediCompli Solution combines Quality System Documents with FDA 21 CFR 11 Compliant Document Approval Workflows for medical device companies.

It is a highly secure solution based on ISO 13485, IEC 62304, ISO 14971 and FDA 21 CFR 820, FDA 21 CFR 11.

Set on Confluence with integrated software modules configured specifically for the medical devices industry, it is the combined creation of SoftComply, Comalatech, and Clearvision.

SoftComply automates regulatory compliance for medical device manufacturers with their Atlassian apps — the SoftComply eQMS on Confluence and the SoftComply Risk Manager apps on Jira. Comalatech is a developer of innovative and powerful collaboration tools on the Atlassian Marketplace, developing apps for both Confluence and Jira. And Clearvision is an Atlassian Platinum Solution Partner, providing an array of services which cater to the Atlassian Stack and other collaboration applications including consultancy, training and support. Their bespoke cloud solution, ClearHost, provides a highly secure environment for the applications in question.

To become compliant with ISO 13485, IEC 62304, ISO 14971 and 21 CFR 820, users need to add their company and product development details.

MediCompli was created as a result of the challenges faced by medical device software teams where building Quality System Documentation was concerned. A good Quality Management System (QMS) provides the necessary foundation for software innovation, but teams striving for a CE mark in the EU, or FDA approval in the United States must meet stringent compliance requirements.

The purpose of a QMS is to guarantee that a product developed by the company is safe and effective to satisfy the needs of the user with an acceptable level of risk. As such, the Quality System Documents describe in detail the planning, design and development of a medical device, as specified in the criteria for ISO 13485, ISO 14971, IEC 62304 and FDA 21 CFR 820.

MEDICOMPLI ADHERES TO THE FOLLOWING SECURITY REQUIREMENTS AS OUTLINED BY FDA 21 STANDARDS:

Standards
11.10 (b)Documents must be made available for auditors in human-readable and electronic formats.
11.10 (d)System access must be limited to authorised individuals.
11.10 (g)Use of authority checks to ensure that only authorised individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record or perform the operation at hand.
11.10 (k)(1)Use of appropriate controls over systems documentation including:1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of system documentation.
11.200 (a)(1)Electronic signatures shall employ at least two distinct identification components, such as an identification code and password.

- Document Approval: 11.10 (k) (1) Specifies the need for control over the revision and change of documents inside the QMS. The only feasible way to add this in is with a formal approval process that prevents documents from being published unless signed off.

- E-Signatures: FDA 21 CFR 11 clearly states that electronic records systems must employ electronic signatures in approvals. The 11.200 (a)(1) standard clarifies even further that e-signatures must utilise two distinct identification components, such as a username and password. This means it is not enough to have team members write 'approved' on quality documents, as they must be electronically signed in order to be compliant.

- Access Control: The document control system doesn't offer much control if anyone can access it. That's why access control is a critical piece of compliant digital QMS repositories. By limiting users that can interact with and publish documents, the finished content is more trustworthy.

Each of these features helps teams meet a critical component of FDA 21 CFR 11 compliance, but they are not part of common software tools, such as Word. That's why MediCompli was developed.

There is no other solution in the hands of medical device software teams managed on an AWS Server that combines the power of Confluence with the features required by software teams to reach compliance with ISO standards or FDA guidelines.

While only some clauses of 21 CFR 11 have been listed, MediCompli pracitices all those that are applicable.

CONCLUSION

Data protection is a primary design consideration for the infrastructure, products and personal operations of MediCompli.

MediCompli, along with AWS, offers a level of protection that very few public cloud providers or IT teams are able to match. Protecting data is core to our business, and as such, we've invested heavily in security, resources and expertise. We hope that this goes a long way in instilling faith in our customers as we free them to focus on their business and innovation.

MediCompli simplifies building documentation. Watch our short demo for more insight.