Privacy & Security Whitepaper for

EU Cloud Platform for Medical Software Solutions

Editor:	Digital Services Operations Fresenius Medical Care Deutschland GmbH Else-Kröner-Str. 1 D - 61352 Bad Homburg v.d.H. Phone: +49 (0) 6172-609-7000 Mail: digital.services.EMEA@freseniusmedicalcare.com

FRESENIUS MEDICAL CARE

Table of Contents

1. Introduction 3
1.1 Applications 3
2. Data Privacy and Data Protection 3
3. People Security 3
3.1 Awareness Trainings 3
3.2 Background Checks 4
3.3 Employee Education 4
4. Operational Security 4
4.1 Security of Data 4
4.2 Access Control 4
4.3 Internal Credential Policy 4
4.4 Secrets Management 4
4.5 Data Encryption 4
4.6 Endpoint Security protection 4
4.7 Vulnerability management 5
4.8 Penetration Testing 5
4.9 Monitoring 5
5. Physical Security 5
5.1 Office Security 5
5.2 Datacenter Security 5
6. Business Continuity 5
6.1 Business Continuity Plan 5
6.2 Disaster Recovery 6
6.3 Incident Response Plan 6
6.4 Vendor Management 6
7. Regulatory Compliance 6
7.1 Data Transfer Attestation for HDS 6

1. Introduction

This document describes the security aspects in operation and deployment of the Fresenius Medical Care EU Cloud Platform. The platform is the operational foundation for Fresenius Medical Care's cloud-based business solutions and enables the delivery of basic and advanced IT-based services and solutions to clinics and patients within EU.

The secure, stable and legally compliant operation is the basis for these new types of cloud service solutions. Reliable operation is mission critical for Fresenius Medical Care and its customers and must be highly available within the geographical area. Our cloud services are designed to deliver better security than many traditional on-premises solutions. We have security as a priority to protect our own operations. The protection of our cloud services and IT environment is our focus in business.

1.1 Applications

The applications and solutions are built on a secure platform and its high-protected services. Therefore, application-specific topics are excluded and not part of this document.

EMEA development units will follow an internal standard operating procedure (SOP) “Secure Coding Policy” which is based on a risk-based approach utilizing ISO 27001 methods and controls.

Security is implemented by design and follows industrial standards and best practices. Furthermore Cybersecurity and Risk Assessment are part of the development process and operational concept.

2. Data Privacy and Data Protection

The platform service provides an environment for applications to run. Please refer to the application security documentation. The productive system is supported exclusively from the EU. Any access to our customers' data is logged and only happens on a transaction-by-transaction basis. Data location and operational team are in EU.

Fresenius Medical Care take steps to protect the privacy of our customers and limit excessive requests while meeting our legal obligations. GDPR is implemented by design under involvement of Data Privacy Officer and legal team. Protecting the privacy and security of the data you store on the Fresenius Medical Care Cloud is our priority while we comply with these legal requests.

3. People Security

3.1 Awareness Trainings

Fresenius Medical Care employees are trained on company policies and security practices. This includes annual security training and on-going security awareness updates and related activities. All new Fresenius Medical Care employees certify their agreement to comply with Fresenius Medical Care information security policies and attend cyber security training during the onboarding process. In addition, all Fresenius Medical Care employees must take and pass the privacy training, which covers privacy best practices and compliance requirements under applicable privacy law, including the General Data Protection Regulation (GDPR).

3.2 Background Checks

The hiring process for candidates at Fresenius Medical Care includes external reference checks. These checks may also include verification of education and previous employment history.
Where local labor law or statutory regulations permit, Fresenius Medical Care may also conduct criminal, credit, immigration and security checks, depending upon the specific jurisdiction and position.

3.3 Employee Education

Fresenius Medical Care maintains ongoing communication regarding emerging threats and regularly informs employees about phishing campaigns. Employees are instructed to promptly report any suspected security incidents to the Information Security or Information Technology departments.

4. Operational Security

4.1 Security of Data

Protecting customer data is of utmost importance to Fresenius Medical Care. To ensure this, servers are secured with multilayered security controls and regularly undergo vulnerability scans. All services employ encrypted backups, and servers use up-to-date Transport Layer Security (TLS) encryption to safeguard data transmitted over the internet and public networks.

4.2 Access Control

To keep data private and secure, we logically isolate customer's data from that of other customers and users, even when it's stored on the same physical server. Only a small group of administrative employees have access to customer data. For employees, access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know to match access privileges to defined responsibilities. Employees are only granted a limited set of default permissions to access company resources.

4.3 Internal Credential Policy

Fresenius Medical Care's internal credential policy governs the creation, protection and frequency of credential changes. Credential complexity is in line with industry standard practices (e.g. long password, high complexity, lockout policy, etc. as part of our AD implementation). Credentials are transmitted via a hypertext transfer protocol secured (HTTPS) connection. Fresenius Medical Care uses its Privileged Access Security Solution to manage, control, audit and rotate credentials.

4.4 Secrets Management

Fresenius Medical Care follows best practices for managing secrets and uses a combination of tools that have proven to be secure and scalable, which is complemented by our password retention policy.

4.5 Data Encryption

Customers will benefit from solid end-to-end TLS encrypted connections that are implemented by design in our platform. Data in transit (e.g., using SSL, VPN, HTTPS) and data at rest are always encrypted using state-of-the-art methods.

4.6 Endpoint Security protection

Malware attacks can result in account compromise, data theft, and unauthorized network access. Fresenius Medical Care treats these threats with the utmost diligence and employs a range of strategies

to prevent, detect, and eliminate malware. Servers and employee workstations are safeguarded with antivirus software and adhere to industry best practices.

4.7 Vulnerability management

The vulnerability management process actively identifies security threats through a combination of commercially available tools and in-house methods, thorough automated and manual penetration testing, quality assurance procedures, software security reviews, and external audits.

4.8 Penetration Testing

Fresenius Medical Care conducts regular penetration testing through both an internal operational team and external third-party vendors. By leveraging advanced penetration testing tools, the company gains a comprehensive understanding of existing vulnerabilities and attack vectors, enabling effective risk mitigation against cyberattacks.

4.9 Monitoring

Monitoring focuses on data collected from internal network traffic, employee activities on systems, and external vulnerability intelligence. Throughout our global network, anomaly detection systems are deployed to identify suspicious behaviors, including unusual traffic patterns or potentially malicious connections.

5. Physical Security

5.1 Office Security

The physical security of Fresenius Medical Care offices and facilities is established and implemented in strict accordance with the company's security standards, ensuring protection of infrastructure against natural disasters, accidents, and malicious threats. Clearly defined security perimeters and operational procedures safeguard areas housing sensitive or critical information within information processing centers. Entry points are strictly controlled through the use of physical badges and access cards to prevent unauthorized access, with continuous monitoring provided by security personnel and surveillance cameras.

5.2 Datacenter Security

Fresenius Medical Care´s data centers are geographically distributed and employ a variety of physical security controls. The facilities comply with industry-leading standards for physical and environmental controls. Fresenius Medical Care utilizes Microsoft Azure for its production systems, adhering to standardized industry best practices.

6. Business Continuity

6.1 Business Continuity Plan

Fresenius Medical Care maintains formal business continuity and disaster recovery plans, which are regularly reviewed and updated. The company has developed a robust business continuity strategy that allows for rapid response and sustained resilience in the face of various disruptions, including natural disasters and system failures.

6.2 Disaster Recovery

Fresenius Medical Care implements a disaster recovery program that is distributed across the organization. To prevent data loss, Fresenius Medical Care performs ongoing data replication and backup within each data center. Fresenius Medical Care maintains a disaster recovery facility, which enables consistent service performance and minimal data loss in the event of a natural disaster or system failure.

6.3 Incident Response Plan

Fresenius Medical Care maintains a formalized incident response plan (IRP) and policy. The incident response policy defines how security incidents are identified, classified, reported, remediated and mitigated throughout incident response stages including post-incident assessments. The Fresenius Medical Care information security department promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level.

6.4 Vendor Management

The Fresenius Medical Care information security department evaluates potential vendors using a vendor qualification risk assessment process and maintains ongoing oversight of vendors to meet Fresenius Medical Care's information security standards.

7. Regulatory Compliance

Our customers have varying compliance requirements. Our customers operate primarily in medical device and treatment providing regulated environments. Fresenius Medical Care takes care and provides the necessary certifications and complies with the necessary regulatory measures to provide trouble free operations of services provided by our solutions.

Basic cloud operations include ISO 27001, ISO 27002, ISO 27017, ISO 27018 and HDS (France) as the basis for infrastructure operation and underlying Cloud Service Providers. Fresenius Medical Care is compliant to law regulations in EU.

7.1 Data Transfer Attestation for HDS

Fresenius Medical Care does not transfer personal health data to a country outside the European Economic Area.