RehaCom® Online Security White Paper

1. Introduction

Health data belongs to the category of particularly sensitive personal data within the meaning of the GDPR. Its processing requires an especially high level of protection – particularly in the therapeutic context, where it forms the basis of every treatment. For us, this means that information security and data protection are not secondary obligations, but are integrated into our products from the outset as fundamental design principles. Our goal is to provide all parties with the highest possible level of protection at all times.

With RehaCom®, we have been providing an internationally established system for computer-aided cognitive rehabilitation since the early 1990s, used in clinics, rehabilitation centers, and practices worldwide. With RehaCom® Online, we have transferred this long-standing expertise into a modern, web-based platform that enables therapists and patients to work securely and flexibly from any location.

RehaCom® Online addresses:

1. a growing demand for location- and device-independent working – both for therapists maintaining care structures across multiple sites, and for patients undergoing training in inpatient, outpatient, or home rehabilitation,
2. new expectations from our customers regarding integration with modern software products and technologies, as well as
3. the technological necessity of migrating classic training and diagnostic modules to a modern, browser-based, and platform-independent architecture.

With RehaCom® Online, our product evolves from a purely locally installed application to a cloud-based care system. This transformation not only expands the possibilities for facilities and patients, but also increases our responsibility to make the security of our systems transparent, traceable, and verifiable.

This white paper provides a structured overview of our security architecture and our principles in the areas of cyber and information security for RehaCom® Online. It is addressed to our customers, technology partners, and all those who wish to form a well-founded and comprehensible picture of how we anchor information security at HASOMED both organizationally and technically.

Our commitment is clear: security is not created through declarations or promises, but through clearly defined processes and principles, robust measures, and continuous improvement. This document is an expression of this stance – and explicitly invites critical scrutiny and professional dialogue.

2. Architecture & Operating Model

2.1 Cloud-Native SaaS Architecture

RehaCom® Online is provided as Software-as-a-Service and operated entirely in the cloud. Therapists and patients access the platform via a secured web interface – without local installation, without dedicated practice infrastructure, and without device-specific dependencies.

The architecture follows a modular approach with a clear separation of frontend, backend, and data management. It is designed for scalability, security, and high availability, and primarily uses Platform-as-a-Service components to minimize maintenance efforts, attack surfaces, and operational risks. Production and test environments are strictly separated both technically and organizationally.

Sensitive system resources are accessible exclusively via private network paths. Public IP addresses are not used for backend services; network segmentation is implemented through virtual networks and fine-grained access rules. Changes to the infrastructure are centrally managed, versioned, and documented in a traceable manner.

All operations take place in certified data centers in Germany. Patient data does not leave the German legal jurisdiction.

2.2 Core Components

The architecture of RehaCom® Online encompasses the typical layers of a modern SaaS application. They are designed so that each component fulfills a clearly defined role, with security and availability requirements addressed throughout.

Application Layer

- **Web Frontend**: Browser-based interfaces for therapists and patients, optimized for secure and responsive use both in the facility and in home rehabilitation.
- **Training Engine**: A browser-executed engine that provides cognitive training modules in a platform-independent manner and controls them through the web interface.

Backend Layer

- **Application Services**: Modularly structured services encapsulating therapy planning, module configuration, evaluations, and interfaces.
- **API Gateway**: The central, secured entry point for all requests from the web frontends.

Data and Platform Layer

- **Tenant-Specific Data Storage**: Patient and therapy data – including diagnoses, training histories, and cognitive test results – are stored encrypted in a relational database (Azure Database for PostgreSQL Flexible Server) using Transparent Data Encryption (TDE). Each facility has a logically separated data area.
- **Key Management**: Cryptographic key material is managed centrally with role-based access control in a dedicated key management service (Azure Key Vault).
- **Backup and Recovery**: Automated backups, regularly tested recovery procedures, and defined recovery time objectives form the backbone of our availability and contingency architecture.
- **Observability**: Security and operational events are centrally recorded, logged for 90 days, and continuously analyzed.

2.3 Shared Responsibility Model

The secure processing of sensitive health data requires not only technical measures, but also a clear organizational division of responsibilities. In the case of RehaCom® Online, this division follows the roles of HASOMED GmbH and the using facilities and therapists.

Responsibility of HASOMED GmbH

HASOMED GmbH is the manufacturer and provider of RehaCom® Online and the sole contractual partner of the using facilities and therapists. It bears overall responsibility for the design, legal classification, and compliance of the product – particularly with the requirements of the GDPR and the European Medical Device Regulation (MDR) – as well as for the cyber and information security of RehaCom® Online.

Within the framework of data processing on behalf of others pursuant to Art. 28 GDPR, HASOMED GmbH is responsible for the secure operation and further development of the platform: cloud infrastructure, encryption and access control mechanisms, vulnerability management, the selection and oversight of sub-processors, and the maintenance of data processing agreements (DPA) with using facilities. All of this is embedded in our ISO/IEC 27001 certified Information Security Management System (ISMS), which is verified through regular internal and external audits that verify the effectiveness of our security measures. In the event of a security incident, HASOMED GmbH is the central point of contact for its customers and coordinates, where necessary, with the relevant supervisory authorities.

Responsibility of Using Facilities and Therapists

The using facilities and individual therapists are, in relation to HASOMED GmbH, data controllers within the meaning of Art. 4 No. 7 GDPR. They are responsible in particular for the lawful collection of patient consent, the selection of data to be processed, and compliance with their professional obligations.

On the technical side, the protection and maintenance of the devices used, a secure network configuration, and responsible handling of access credentials are their responsibility. These tasks lie outside the direct sphere of influence of HASOMED GmbH. However, we actively support our customers with practical guidance and assistance to ensure that local protective measures work in concert with the overall architecture.

Patients use RehaCom® Online exclusively to the extent that they have been activated and provided with training by their treating therapists. The complexity of the platform is intentionally kept low for them: authentication, training execution, and synchronization of results are largely automated in a guided process.

3. Risk Mitigation Measures

3.1 Our Core Principles

The security architecture of RehaCom® Online is based on clearly defined guiding principles. These form the binding framework for all decisions in the field of information security and thus lay the foundation for consistent, verifiable security management.

It is important to us not to regard security as a collection of individual technical measures, but as a management task supported by overarching values, binding rules, and a lived security culture. We deliberately make these principles transparent because we are convinced that lasting security can only be achieved through traceable decisions and clear responsibilities.

Anticipate Rather Than React

A central principle of our security program is to address risks proactively and strategically. We work with scenarios that help us make threats tangible and derive concrete measures from them. Ohelfen, Bedrohungen nly risks that are clearly identified can be effectively countered with solutions.n.

In doing so, we emphasize various dimensions, for example:

- **Information & Data:** What attack scenarios apply to the sensitive data we process?
- **Technology Stack:** What realistic threats arise for our systems and infrastructure?
- **Market & Customers:** What security expectations exist, and how do we translate them into measures?
- **Our Own Risk Appetite:** What initiatives and measures follow from our self-understanding and our defined risk framework?

This multi-dimensional perspective makes security for us **discussable, prioritizable and plannable** – and thus forms the basis for continuously developing our security program.

Transparency & Traceability

Security must always be traceable for us – not merely a promise. We therefore document our security concept openly, provide context, and invite critical review. We believe that trust and security arise from dialogue. Notices of vulnerabilities, suggestions for improvement, or technical questions are therefore actively taken up – among other channels, via our Security Contact Point and within the framework of our Bug Bounty Program.

Security as a Default Principle

Security in RehaCom® Online is not an optional add-on, but a mandatory, integral part of our system architecture from the very beginning. Fundamental protective mechanisms such as encryption, access controls, and tenant separation are implemented by default and cannot be disabled or made dependent on individual decisions.

This fundamental stance reflects our sense of responsibility towards the using facilities and the particularly sensitive health data they process.

Alignment with Standards and Established Principles

We rely on proven architectural principles, clear responsibilities, and the targeted use of modern security technologies. We do not reinvent security, but align ourselves with established standards and recognized best practices – including the recommendations of the German Federal Office for Information Security (BSI), the C5 requirements catalogue, and common cloud security frameworks.

HASOMED GmbH operates an Information Security Management System (ISMS) certified to ISO/IEC 27001, in which RehaCom® Online is fully embedded. The ISMS defines binding processes, roles, and control mechanisms for all security-relevant activities. Within the framework of the ISMS, we regularly undergo internal and external audits that verify the effectiveness of our security measures and ensure their continuous development.

In this way, we create a robust and traceable security architecture whose implementation is not only documented internally, but also regularly confirmed by independent auditors.

3.2 Technical Measures

Encryption of Sensitive Data

In RehaCom® Online, all sensitive content – including diagnoses, training histories, cognitive test results, therapy plans, and progress documentation – is consistently processed and stored in encrypted form.

Technically, this occurs on multiple levels:

- **Encryption of Stored Data:** All content stored in the database is encrypted at the storage level using AES-256. Documents and files processed as part of therapy are also stored in encrypted form.
- **Encryption in Transit:** All connections between the devices of therapists or patients and our platform, as well as between the internal components of our architecture, are conducted exclusively via TLS 1.2 or higher.
- **Centralized Key Management:** The cryptographic key material used is managed in a dedicated key management service (Azure Key Vault). Access to keys is exclusively role-based via Managed Identities and is fully logged.
- **Tenant Separation:** The data of individual facilities is logically separated from one another; technical and organizational tenant separation prevents data from different customers from being commingled.

For the using facilities, this means: patient data is consistently protected cryptographically both in storage and in transit, and access to the key material used follows a strict, traceable authorization model.

Multi-Layered Security Concept for Workplace, Infrastructure, and Application Levels

In addition to the specific protective mechanisms within RehaCom® Online, we operate a multi-layered security concept to safeguard both our corporate IT and the underlying technical infrastructure. Our approach covers all relevant levels – from the workplace through the server and network infrastructure to application security – and is regularly reviewed and further developed within the framework of our ISO/IEC 27001 certified Information Security Management System (ISMS). The cloud-based system components are additionally audited in accordance with the C5 standard (Cloud Computing Compliance Criteria Catalogue) of the BSI.

Workplace:

At the workplace level, we rely on a secured enterprise browser as the central access point to internal systems, a central identity provider (IdP) with integrated password and device management, as well as secure collaboration and communication tools.

These components ensure that access to internal systems is controlled, traceable, and bound to central authentication and authorization requirements.

Infrastructure:

To secure our centrally operated systems, we rely on specialized cloud security solutions, including in particular Cloud Native Application Protection Platforms (CNAPP) and Cloud Infrastructure Entitlement Management (CIEM). These solutions continuously monitor configurations, permissions, and resource accesses, detect deviations from defined security policies at an early stage, and prevent unauthorized access. This ensures that our systems are operated at all times on a robust and compliant basis, even in dynamic operating environments.

The cloud-based components are additionally audited in accordance with the C5 standard (Cloud Computing Compliance Criteria Catalogue) of the BSI, in order to have compliance with the highest security and compliance requirements regularly confirmed by independent auditors.

Application Security:

Application security is ensured through systematic vulnerability management, automated security-relevant tests, regular penetration tests, and a Bug Bounty Program. These measures make it possible to identify potential vulnerabilities at an early stage and to continuously incorporate security requirements into development processes.

3.3 Organizational Measures

Professional Security Program with CISOIQ

Security is for us not merely a technical matter, but a fixed component of our organization. From the outset, we have established an independent security program firmly anchored in our corporate structure through the role of a Chief Information Security Officer (CISO).

For the planning, implementation, and ongoing supervision of our security program, we work with **CISOIQ**, a specialized Berlin-based cyber security company. CISOIQ not only fulfills advisory roles, but also operates with its own expert staff to implement our security program – for example in designing policies, establishing security-relevant processes, operational vulnerability management, and preparation for internal and external audits.

The CISOIQ security team is closely integrated into our organization, works in continuous coordination with the management of HASOMED GmbH, and reports directly to the executive leadership. This ensures that cyber and information security at

HASOMED is not treated as a peripheral topic, but as an ongoing process closely intertwined with the technological development of RehaCom® Online.

Security Awareness & Culture in the Team

For us it is clear: security is not the task of individual specialists alone, but a shared responsibility of all employees. Each and every person contributes to honoring the trust that customers and market participants place in us.

That is why awareness and a culture of responsibility have been a key pillar of our security program from the very beginning. We promote this through regular awareness training, clear guidelines for handling sensitive data, and practical exercises, for example on phishing or password security.

This ensures that security does not remain merely a technical matter, but is a lived part of our corporate culture – and is naturally taken into account in all areas, from product development to day-to-day collaboration.

Four-Eyes Principle for Security-Critical Changes

In the software development of RehaCom® Online, as with all other systems and infrastructure, the following applies: no security-relevant change may be carried out by a single person without oversight.

We therefore combine modern development and operational principles such as consistent versioning, the mandatory four-eyes principle for security-critical changes, and dedicated security reviews by qualified team members. Every change to code, infrastructure, or configuration thus goes through multiple control steps before taking effect in production.

We trust our teams – and at the same time follow the principle that it is good practice to jointly safeguard important steps. This ensures that errors or vulnerabilities do not go unnoticed and that multiple perspectives always feed into security-relevant decisions.

Continuous Penetration Testing

In order to identify potential vulnerabilities at an early stage, we combine various testing methods rather than relying exclusively on standardized procedures.

On one hand, we regularly conduct structured penetration tests that assess, based on defined testing categories, whether publicly accessible systems or applications have potential vulnerabilities. These tests provide us with a systematic and reliable picture of the current security status of our systems.

In addition, we operate a Bug Bounty Program. Here, our platform is continuously tested by a large number of independent security researchers who, using various approaches

and expert perspectives, uncover potential vulnerabilities that are not captured in classical tests.

In addition, we deploy automated analysis tools that continuously search for security-relevant patterns and deviations, thereby continuously monitoring our attack surface.

We are aware that errors can never be completely ruled out. Through the combination of these procedures, however, we ensure that we are able to counter potential attacks at an early stage – both through structured internal reviews and through the continuous incorporation of external perspectives.

Security Audits for Suppliers, Third Parties, and Sub-Processors

For the operation of complex systems, the use of external sub-processors (e.g. for hosting and operations) as well as further third parties, such as manufacturers of software components, frameworks, or libraries, is technically necessary. This involvement requires, however, that we can rely unreservedly on the security level of all parties involved.

Sub-processors within the meaning of Art. 28 GDPR are carefully vetted by HASOMED GmbH before deployment and integrated into data processing agreements. This includes in particular the assessment of their information security level, the review of relevant certifications (e.g. ISO/IEC 27001, C5, SOC 2), and regular audits within the framework of our Information Security Management System (ISMS).

We limit the number of sub-processors used to the necessary minimum and inform our customers transparently about all changes. An up-to-date list of all sub-processors is made publicly available.

For other suppliers and third parties, where no processing on behalf of others takes place (e.g. software libraries or hardware suppliers), we conduct structured due diligence reviews. In doing so, we consider not only formal evidence, but also organizational aspects, such as:

- What security organization is in place?
- What are the processes in the areas of incident response or vulnerability management?
- How transparently do the providers communicate about vulnerabilities or security incidents?
- Does the overall picture meet the requirements for a robust security culture?

This ensures that we apply a consistently high standard throughout the entire supply chain – regardless of whether it concerns sub-processors or other third parties.

Structured Incident Response and Communication Processes

Even with the best possible preparation, security incidents can never be completely ruled out. What is decisive, therefore, is how quickly and in a coordinated manner a response is given. For this reason, we have established clear incident response processes at HASOMED that systematically link technical analysis, internal coordination, and external communication.

Our processes follow defined steps – from initial detection through assessment and containment to lasting remediation and documentation. The roles involved at each stage and the escalation pathways are clearly defined. A particular emphasis is placed on clear communication: both internally between the teams involved and externally towards affected customers and – where necessary – towards supervisory authorities.

In addition, we also consider so-called „near miss situations" – events that could potentially have become critical, but were identified and defused at an early stage. These cases are systematically incorporated into our learning processes. Our goal is not only to handle incidents efficiently, but to make the organization stronger and more resilient in the long term through this process.

Our security approach thus follows the principle of anti-fragility: every disruption or challenge is for us an opportunity to improve structures and processes. This creates a system that not only withstands threats, but continuously adapts to and grows stronger from new ones.

For our customers, this means: in the unlikely event of a security incident, they can rely on HASOMED responding quickly, in a structured manner, and openly – and that every incident leads to even greater strength in the overall system.

4. Legal Admissibility & Compliance

Handling (US) Government Requests

The public debate about possible access by foreign authorities to data stored in the cloud – for example in the context of the **US CLOUD Act** – demonstrates how important technical and organizational sovereignty is in cloud architectures. The US CLOUD Act provides that US authorities can, in certain cases, compel cloud providers with US ownership to disclose data. Such access requires a judicial order from a US federal court and in practice occurs only in very rare exceptional cases. Nevertheless, we explicitly take this risk into account in our architecture and processes:

- RehaCom® Online is **operated exclusively in certified data centers in Germany**. Patient data does not leave the German legal jurisdiction.
- All stored data is **encrypted with AES-256**, and access to the key material used follows a strict, role-based authorization model that is comprehensively logged.

- **Requests from foreign authorities** without a valid German or European legal basis are rejected as a matter of principle.
- **Requests from German authorities** are carefully reviewed by management and our legal department, coordinated with the relevant supervisory authorities, and – where personal data is involved – processed with the involvement of the affected customers.
- To the extent legally permissible, we inform affected customers about government access so that they can exercise their own rights of objection and legal remedies.

This ensures that government access occurs exclusively on the basis of applicable German and European law and that the rights of our customers are protected at all times.

Certifications & Standards

Our security architecture and organizational measures are aligned with established international standards and are regularly reviewed externally.

- The **HASOMED GmbH** is certified to **ISO/IEC 27001** – the internationally recognized standard for Information Security Management Systems (ISMS). The certification scope explicitly also covers the development and provision of web-based software solutions in the healthcare sector. RehaCom® Online is thereby fully embedded in the ISMS and its control mechanisms.
- RehaCom® Online is additionally attested under the **C5 standard (Cloud Computing Compliance Criteria Catalogue)** of the German Federal Office for Information Security (BSI). C5 ensures that cloud services are operated in accordance with transparent, high security criteria.
- RehaCom® Online is conformity-assessed as a **CE-certified Class I medical device** in accordance with the European Medical Device Regulation (MDR). The underlying quality management processes are also embedded in a quality management system (QMS) maintained in accordance with ISO 13485.

We consider ourselves obligated to maintain these certifications and conformity assessments on a permanent basis and to renew them regularly. For our customers, this means that our security measures are not only defined internally, but are also **confirmed by independent external auditors**.

GDPR Compliance

Compliance with the European General Data Protection Regulation (GDPR) is a matter of course for us – it forms the legal basis for every processing of personal data. What is important to us is not merely to formally satisfy the requirements of the GDPR, but to build them into our architecture and processes „by design".

Core principles such as data minimization, purpose limitation, transparency, integrity, confidentiality, and the protection of the rights of data subjects are understood by us not merely as legal requirements, but as practical guidelines for our day-to-day handling of sensitive health data.

Thus the GDPR is for us more than a regulatory framework: it is a design principle that we consistently translate into technology, organization, and processes.

5. Collaboration and Outlook

Security is for us not a completed state, but a shared task that is continuously evolving. This white paper is therefore intended not only to provide insight into our current principles and measures, but also to invite discussion.

We wish to be open about how we understand security at HASOMED, and welcome feedback, criticism, and suggestions. We are convinced: only through constructive exchange with our users, partners, and the specialist public can we continuously improve our security level and together shape reliable digital care in neurorehabilitation.