RehaCom® Online Security White Paper

1. Einleitung

Gesundheitsdaten zählen zu den besonders schutzbedürftigen personenbezogenen Daten im Sinne der DSGVO. Ihre Verarbeitung erfordert ein besonders hohes Schutzniveau – insbesondere im therapeutischen Kontext, indem sie die Grundlage jeder Behandlung bilden. Für uns bedeutet das, dass Informationssicherheit und Datenschutz keine nachgelagerten Pflichten sind, sondern von Anfang an als grundlegende Designprinzipien in unsere Produkte integriert werden. Unser Ziel ist es, allen Beteiligten zu jeder Zeit das höchstmögliche Schutzniveau bereitzustellen.

Mit RehaCom® stellen wir seit den frühen 1990er Jahren ein international etabliertes System für die computergestützte kognitive Rehabilitation bereit, das in Kliniken, Rehazentren und Praxen weltweit eingesetzt wird. Mit RehaCom® Online haben wir diese langjährige Erfahrung in eine moderne, webbasierte Plattform überführt, die Therapeut:innen und Patient:innen eine ortsunabhängige, sichere und flexible Nutzung ermöglicht.

RehaCom® Online bedient:

1. eine wachsende Nachfrage nach orts- und geräteunabhängigem Arbeiten – sowohl für Therapeut:innen, die Versorgungsstrukturen über mehrere Standorte hinweg aufrechterhalten, als auch für Patient:innen, die in stationärer, ambulanter oder häuslicher Rehabilitation Trainings absolvieren,
2. neue Erwartungen unserer Kund:innen an die Integration mit modernen Softwareprodukten und Technologien, sowie
3. die technologische Notwendigkeit, klassische Trainings- und Diagnostikmodule auf eine moderne, browserbasierte und plattformunabhängige Architektur zu überführen.

Mit RehaCom® Online wandelt sich unser Produkt von einer rein lokal installierten Anwendung hin zu einem cloudbasierten Versorgungssystem. Dieser Wandel erweitert nicht nur die Möglichkeiten für Einrichtungen und Patient:innen, sondern erhöht auch unsere Verantwortung, die Sicherheit unserer Systeme transparent, nachvollziehbar und überprüfbar zu gestalten.

Dieses White Paper gibt einen strukturierten Einblick in unsere Sicherheitsarchitektur und unsere Grundsätze im Bereich Cyber- und Informationssicherheit für RehaCom® Online. Es richtet sich an unsere Kund:innen, an Technologiepartner sowie an alle, die sich ein fundiertes und nachvollziehbares Bild davon machen möchten, wie wir Informationssicherheit bei HASOMED organisatorisch und technisch verankern.

Unser Anspruch ist klar: Sicherheit entsteht nicht durch Erklärungen oder Versprechen, sondern durch klar definierte Prozesse und Prinzipien, belastbare Maßnahmen und kontinuierliche Weiterentwicklung. Dieses Dokument versteht sich als Ausdruck dieser Haltung – und lädt ausdrücklich zur kritischen Betrachtung und zum fachlichen Dialog ein.

2. Architektur & Betriebsmodell

2.1 Cloud-native SaaS-Architektur

RehaCom® Online wird als Software-as-a-Service bereitgestellt und vollständig in der Cloud betrieben. Therapeut:innen und Patient:innen greifen über einen gesicherten Webzugang auf die Plattform zu – ohne lokale Installation, ohne dedizierte Praxisinfrastruktur und ohne gerätespezifische Abhängigkeiten.

Die Architektur folgt einem modularen Ansatz mit klarer Trennung von Frontend, Backend und Datenhaltung. Sie ist auf Skalierbarkeit, Sicherheit und hohe Verfügbarkeit ausgelegt und nutzt überwiegend Platform-as-a-Service-Komponenten, um Wartungsaufwände, Angriffsflächen und Betriebsrisiken zu minimieren. Produktions- und Testumgebungen sind technisch und organisatorisch strikt voneinander getrennt.

Sensible Systemressourcen sind ausschließlich über private Netzwerkpfade erreichbar. Öffentliche IP-Adressen werden für Backenddienste nicht verwendet, die Netzwerksegmentierung erfolgt über virtuelle Netzwerke und feingranulare Zugriffsregeln. Änderungen an der Infrastruktur werden zentral verwaltet, versioniert und nachvollziehbar dokumentiert.

Der gesamte Betrieb erfolgt in zertifizierten Rechenzentren in Deutschland. Patientendaten verlassen den deutschen Rechtsraum nicht.

2.2 Kernkomponenten

Die Architektur von RehaCom® Online umfasst die typischen Schichten einer modernen SaaS-Anwendung. Sie sind so gestaltet, dass jede Komponente eine klar umrissene Aufgabe übernimmt und Sicherheits- sowie Verfügbarkeitsanforderungen durchgängig adressiert werden.

Anwendungsschicht

- **Web-Frontend**: Browserbasierte Oberflächen für Therapeut:innen und Patient:innen, optimiert für den sicheren und reaktionsschnellen Einsatz in der Einrichtung wie auch in der häuslichen Rehabilitation.
- **Trainingsengine**: Eine im Browser ausgeführte Engine, die die kognitiven Trainingsmodule plattformunabhängig bereitstellt und über die Web-Oberfläche steuert.

Backend-Schicht

- **Applikationsdienste**: Modular aufgebaute Dienste, die Therapieplanung, Modulkonfiguration, Auswertungen und Schnittstellen kapseln.
- **API-Gateway**: Zentrale, abgesicherte Eintrittsstelle für sämtliche Anfragen aus den Web-Frontends.

Daten- und Plattformschicht

- **Mandantenspezifische Datenhaltung**: Patienten- und Therapiedaten – einschließlich Diagnosen, Trainingsverläufen und kognitiven Testergebnissen – werden in einer relationalen Datenbank (Azure Database for PostgreSQL Flexible Server) mittels Transparent Data Encryption (TDE) verschlüsselt abgelegt. Jede Einrichtung verfügt über einen logisch getrennten Datenbereich.
- **Schlüsselverwaltung**: Kryptografisches Schlüsselmaterial wird zentral und mit rollenbasierter Zugriffskontrolle in einem dedizierten Key-Management-Dienst (Azure Key Vault) verwaltet.
- **Backup und Wiederherstellung**: Automatisierte Backups, regelmäßig erprobte Wiederherstellungsverfahren und definierte Wiederanlaufzeiten bilden das Rückgrat unserer Verfügbarkeits- und Notfallarchitektur.
- **Beobachtbarkeit**: Sicherheits- und Betriebsereignisse werden zentral erfasst, für 90 Tage protokolliert und kontinuierlich ausgewertet.

2.3 Geteiltes Verantwortungsmodell

Die sichere Verarbeitung sensibler Gesundheitsdaten erfordert nicht nur technische Maßnahmen, sondern auch eine klare organisatorische Verantwortungsverteilung. Im Fall von RehaCom® Online ergibt sich diese entlang der Rollen von HASOMED GmbH und den nutzenden Einrichtungen sowie Therapeut:innen.

Verantwortung der HASOMED GmbH

Die HASOMED GmbH ist Herstellerin und Anbieterin von RehaCom® Online und alleinige Vertragspartnerin der nutzenden Einrichtungen und Therapeut:innen. Sie trägt die Gesamtverantwortung für Konzeption, rechtliche Einordnung und Konformität des Produkts – insbesondere mit den Anforderungen der DSGVO und der europäischen Medizinprodukte-Verordnung (MDR) – sowie für die Cyber- und Informationssicherheit von RehaCom® Online.

Im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DSGVO verantwortet die HASOMED GmbH den sicheren Betrieb und die Weiterentwicklung der Plattform: Cloud-Infrastruktur, Verschlüsselungs- und Zugriffskontrollmechanismen, Schwachstellenmanagement, die Auswahl und Steuerung der Unterauftragsverarbeiter sowie die Pflege der Auftragsverarbeitungsverträge (AVV) mit den nutzenden Einrichtungen. Eingebettet ist all dies in unser nach ISO/IEC 27001 zertifiziertes Informationssicherheits-Managementsystem (ISMS), das durch regelmäßige interne

und externe Audits geprüft wird. Im Falle eines Sicherheitsvorfalls ist die HASOMED GmbH zentrale Kontaktstelle für ihre Kund:innen und stimmt sich, falls erforderlich, mit den zuständigen Aufsichtsbehörden ab.

Verantwortung der nutzenden Einrichtungen und Therapeut:innen

Die nutzenden Einrichtungen sowie die einzelnen Therapeut:innen sind im Verhältnis zur HASOMED GmbH datenschutzrechtlich Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO. Ihnen obliegt insbesondere die rechtmäßige Erhebung der Patient:innen-Einwilligungen, die Auswahl der zu verarbeitenden Daten sowie die Einhaltung ihrer berufsrechtlichen Pflichten.

Auf technischer Seite liegen Schutz und Pflege der genutzten Endgeräte, eine sichere Netzwerkkonfiguration sowie der verantwortungsvolle Umgang mit Zugangsdaten in ihrer Hand. Diese Aufgaben liegen außerhalb des direkten Einflussbereichs der HASOMED GmbH. Wir unterstützen unsere Kund:innen jedoch aktiv mit praxisnahen Hinweisen und Hilfestellungen, um sicherzustellen, dass die lokalen Schutzmaßnahmen mit der Gesamtarchitektur zusammenspielen.

Patient:innen nutzen RehaCom® Online ausschließlich in dem Umfang, in dem sie von ihren behandelnden Therapeut:innen freigeschaltet und mit Trainings versorgt werden. Die Komplexität der Plattform bleibt für sie bewusst gering: Authentifizierung, Trainingsdurchführung und Synchronisation der Ergebnisse erfolgen weitgehend automatisiert in einem geführten Ablauf.

3. Maßnahmen zur Risikominimierung

3.1 Unsere Grundprinzipien

Die Sicherheitsarchitektur von RehaCom® Online beruht auf klar definierten Leitprinzipien. Sie bilden den verbindlichen Orientierungsrahmen für alle Entscheidungen im Bereich Informationssicherheit und schaffen damit die Grundlage für ein konsistentes, überprüfbares Sicherheitsmanagement.

Uns ist wichtig, Sicherheit nicht als eine Ansammlung technischer Einzelmaßnahmen zu begreifen, sondern als eine Managementaufgabe, die durch übergeordnete Werte, verbindliche Regeln und eine gelebte Sicherheitskultur getragen wird. Diese Prinzipien machen wir bewusst transparent, weil wir überzeugt sind, dass nachhaltige Sicherheit nur durch nachvollziehbare Entscheidungen und klare Verantwortlichkeiten entstehen kann.

Antizipieren statt Reagieren

Ein zentrales Prinzip unseres Sicherheitsprogramms ist es, Risiken vorausschauend und strategisch zu adressieren. Wir arbeiten mit Szenarien, die uns helfen, Bedrohungen

greifbar zu machen und daraus konkrete Maßnahmen abzuleiten. Denn nur Risiken, die klar benannt sind, lassen sich auch wirksam mit Lösungen beantworten.

Dabei betonen wir verschiedene Dimensionen, zum Beispiel:

- **Informationen & Daten:** Welche Angriffsszenarien wirken auf die sensiblen Daten, die wir verarbeiten?
- **Technologie-Stack:** Welche realistischen Bedrohungen ergeben sich für unsere Systeme und Infrastruktur?
- **Markt & Kund:innen:** Welche Erwartungen an Sicherheit bestehen, und wie übersetzen wir sie in Maßnahmen?
- **Eigener Risk Appetite:** Welche Initiativen und Maßnahmen folgen aus unserem Selbstverständnis und unserem definierten Risikorahmen?

Diese mehrdimensionale Betrachtung macht Sicherheit für uns **besprechbar, priorisierbar und planbar** – und bildet damit die Grundlage, unser Sicherheitsprogramm kontinuierlich weiterzuentwickeln.

Transparenz & Nachvollziehbarkeit

Sicherheit muss für uns immer auch nachvollziehbar sein – nicht nur ein Versprechen. Deshalb dokumentieren wir unser Sicherheitskonzept offen, schaffen Kontext und laden zur kritischen Überprüfung ein. Wir glauben, dass Vertrauen und Sicherheit aus Dialog entstehen. Hinweise zu Schwachstellen, Verbesserungsvorschläge oder technische Rückfragen greifen wir daher aktiv auf – unter anderem über unseren Security Contact Point und im Rahmen unseres Bug-Bounty-Programms.

Sicherheit als Standardprinzip

Sicherheit ist bei RehaCom® Online kein optionaler Zusatz, sondern ein von Beginn an verpflichtend integriertem Bestandteil unserer Systemarchitektur. Grundlegende Schutzmechanismen wie Verschlüsselung, Zugriffskontrollen und Mandantentrennung werden standardmäßig implementiert und sind nicht abschaltbar oder von individuellen Entscheidungen abhängig.

Diese Grundhaltung ist Ausdruck unseres Verantwortungsbewusstseins gegenüber den nutzenden Einrichtungen und den von ihnen verarbeiteten besonders schutzbedürftigen Gesundheitsdaten.

Orientierung an Standards und bewährten Prinzipien

Wir setzen auf bewährte Architekturprinzipien, klare Verantwortlichkeiten und den gezielten Einsatz moderner Sicherheitstechnologien. Dabei erfinden wir Sicherheit nicht neu, sondern orientieren uns an etablierten Standards und anerkannten Best Practices – unter anderem an den Empfehlungen des Bundesamts für Sicherheit in der

Informationstechnik (BSI), dem C5-Anforderungskatalog sowie gängigen Cloud-Security-Frameworks.

Die HASOMED GmbH betreibt ein nach ISO/IEC 27001 zertifiziertes Informationssicherheits-Managementsystem (ISMS), in das auch RehaCom® Online vollständig eingebettet ist. Das ISMS definiert verbindliche Prozesse, Rollen und Kontrollmechanismen für alle sicherheitsrelevanten Tätigkeiten. Im Rahmen des ISMS durchlaufen wir regelmäßig interne und externe Audits, die die Wirksamkeit unserer Sicherheitsmaßnahmen überprüfen und deren kontinuierliche Weiterentwicklung sicherstellen.

Auf diese Weise schaffen wir eine belastbare und nachvollziehbare Sicherheitsarchitektur, deren Umsetzung nicht nur intern dokumentiert, sondern auch regelmäßig durch unabhängige Prüfer bestätigt wird.

3.2 Technische Maßnahmen

Verschlüsselung sensibler Daten

In RehaCom® Online werden sämtliche sensiblen Inhalte – darunter Diagnosen, Trainingsverläufe, kognitive Testergebnisse, Therapieplanungen und Verlaufsdokumentationen – durchgängig verschlüsselt verarbeitet und gespeichert.

Technisch geschieht dies auf mehreren Ebenen:

- **Verschlüsselung gespeicherter Daten:** Alle in der Datenbank abgelegten Inhalte werden auf Datenträgerebene mit AES-256 verschlüsselt. Dokumente und Dateien, die im Rahmen der Therapie verarbeitet werden, werden ebenfalls verschlüsselt abgelegt.
- **Verschlüsselung im Transport:** Sämtliche Verbindungen zwischen Endgeräten der Therapeut:innen oder Patient:innen und unserer Plattform sowie zwischen den internen Komponenten unserer Architektur erfolgen ausschließlich über TLS 1.2 oder höher.
- **Zentrale Schlüsselverwaltung:** Das eingesetzte kryptografische Schlüsselmaterial wird in einem dedizierten Key-Management-Dienst (Azure Key Vault) verwaltet. Der Zugriff auf Schlüssel erfolgt ausschließlich rollenbasiert über Managed Identities und wird vollständig protokolliert.
- **Mandantentrennung:** Die Daten der einzelnen Einrichtungen sind logisch voneinander getrennt; eine technische und organisatorische Mandantentrennung verhindert, dass Daten unterschiedlicher Kund:innen miteinander vermengt werden können.

Für die nutzenden Einrichtungen bedeutet das: Patientendaten sind sowohl in der Speicherung als auch im Transport durchgängig kryptografisch geschützt, und der Zugriff auf das eingesetzte Schlüsselmaterial folgt einem strikten, nachvollziehbaren Berechtigungsmodell.

Mehrschichtiges Sicherheitskonzept für Arbeitsplatz-, Infrastruktur- und Anwendungsebene

Neben den spezifischen Schutzmechanismen innerhalb von RehaCom® Online betreiben wir ein mehrschichtiges Sicherheitskonzept, um sowohl unsere Unternehmens-IT als auch die zugrunde liegende technische Infrastruktur abzusichern. Unser Ansatz deckt alle relevanten Ebenen ab – vom Arbeitsplatz über die Server- und Netzwerkinfrastruktur bis hin zur Anwendungssicherheit – und wird im Rahmen unseres nach ISO/IEC 27001 zertifizierten Informationssicherheits-Managementsystems (ISMS) regelmäßig überprüft und weiterentwickelt. Die cloudbasierten Systemkomponenten werden zusätzlich nach dem C5-Standard (Cloud Computing Compliance Criteria Catalogue) des BSI auditiert.

Arbeitsplatz:

Auf der Arbeitsplatzebene setzen wir auf einen abgesicherten Enterprise-Browser als zentralen Zugriffspunkt auf interne Systeme, einen zentralen Identity Provider (IdP) mit integriertem Passwort- und Gerätemanagement sowie auf sichere Kollaborations- und Kommunikationstools.

Diese Komponenten stellen sicher, dass der Zugriff auf interne Systeme kontrolliert, nachvollziehbar und an zentrale Authentifizierungs- und Autorisierungsvorgaben gebunden erfolgt.

Infrastruktur:

Für die Absicherung unserer zentral betriebenen Systeme setzen wir auf spezialisierte Cloud-Sicherheitslösungen, darunter insbesondere Cloud Native Application Protection Platforms (CNAPP) sowie Cloud Infrastructure Entitlement Management (CIEM). Diese Lösungen überwachen kontinuierlich Konfigurationen, Berechtigungen und Ressourcenzugriffe, erkennen Abweichungen von definierten Sicherheitsrichtlinien frühzeitig und verhindern unautorisierte Zugriffe. So stellen wir sicher, dass unsere Systeme auch in dynamischen Betriebsumgebungen jederzeit auf einer belastbaren und regelkonformen Grundlage betrieben werden.

Die cloudbasierten Komponenten werden zusätzlich nach dem C5-Standard (Cloud Computing Compliance Criteria Catalogue) des BSI auditiert, um die Einhaltung höchster Sicherheits- und Compliance-Anforderungen regelmäßig durch unabhängige Prüfer bestätigen zu lassen.

Applikationssicherheit:

Die Anwendungssicherheit wird durch ein systematisches Schwachstellenmanagement, automatisierte sicherheitsrelevante Tests, regelmäßige Penetrationstests sowie ein Bug-Bounty-Programm sichergestellt. Diese Maßnahmen ermöglichen es, potenzielle Schwachstellen frühzeitig zu erkennen und Sicherheitsanforderungen laufend in die Entwicklungsprozesse einfließen zu lassen.

3.3 Organisatorische Maßnahmen

Professionelles Sicherheitsprogramm mit CISOIQ

Sicherheit ist für uns nicht nur eine technische Frage, sondern ein fester Bestandteil unserer Organisation. Von Beginn an haben wir ein eigenständiges Sicherheitsprogramm etabliert, das über die Rolle eines Chief Information Security Officers (CISO) fest in unserer Unternehmensstruktur verankert ist.

Für die Planung, Umsetzung und laufende Betreuung unseres Sicherheitsprogramms arbeiten wir mit **CISOIQ**, einem spezialisierten Berliner Cyber-Security-Unternehmen. CISOIQ übernimmt nicht nur beratende Aufgaben, sondern wirkt mit eigenem Fachpersonal operativ an der Umsetzung unseres Sicherheitsprogramms mit — etwa bei der Gestaltung von Richtlinien, dem Aufbau sicherheitsrelevanter Prozesse, dem operativen Schwachstellenmanagement und der Vorbereitung auf interne wie externe Audits.

Das Sicherheitsteam von CISOIQ ist eng in unsere Organisation eingebunden, arbeitet in kontinuierlicher Abstimmung mit dem Management der HASOMED GmbH und berichtet direkt an die Geschäftsführung. Dadurch stellen wir sicher, dass Cyber- und Informationssicherheit bei HASOMED nicht als begleitendes Thema verstanden wird, sondern als kontinuierlicher Prozess, der eng mit der technologischen Entwicklung von RehaCom® Online verzahnt ist.

Sicherheitsbewusstsein & Kultur im Team

Für uns ist klar: Sicherheit ist nicht allein Aufgabe einzelner Spezialist:innen, sondern eine gemeinsame Verantwortung aller Mitarbeitenden. Jede und jeder trägt dazu bei, dem Vertrauen gerecht zu werden, das uns Kund:innen und Marktteilnehmer entgegenbringen.

Deshalb ist Awareness und Verantwortungskultur von Beginn an eine tragende Säule unseres Security-Programms. Wir fördern dies durch regelmäßige Awareness-Trainings, klare Leitlinien im Umgang mit sensiblen Daten und praxisnahe Übungen, etwa zu Phishing oder Passwortsicherheit.

So stellen wir sicher, dass Security nicht nur ein technisches Thema bleibt, sondern ein gelebter Teil unserer Unternehmenskultur ist – und in allen Bereichen, von der Produktentwicklung bis zur täglichen Zusammenarbeit, selbstverständlich berücksichtigt wird.

Vier-Augen-Prinzip bei sicherheitskritischen Änderungen

In der Softwareentwicklung von RehaCom® Online, ebenso wie bei allen anderen Systemen und Infrastrukturen, gilt für uns: Keine sicherheitsrelevante Änderung darf von einer einzelnen Person unkontrolliert durchgeführt werden.

Daher kombinieren wir moderne Entwicklungs- und Betriebsprinzipien wie konsequente Versionierung, das verbindliche Vier-Augen-Prinzip bei sicherheitskritischen Änderungen und dedizierte Security-Reviews durch qualifizierte Teammitglieder. Jede Änderung an Code, Infrastruktur oder Konfiguration durchläuft damit mehrere Kontrollschritte, bevor sie produktiv wirksam wird.

Wir vertrauen unseren Teams – und gleichzeitig folgen wir dem Grundsatz, dass es gute Praxis ist, wichtige Schritte gemeinsam abzusichern. So stellen wir sicher, dass Fehler oder Schwachstellen nicht unbemerkt bleiben und dass immer mehrere Perspektiven in sicherheitsrelevante Entscheidungen einfließen.

Kontinuierliche Penetrationstests

Um mögliche Schwachstellen frühzeitig zu identifizieren, kombinieren wir verschiedene Prüfmethoden, anstatt uns ausschließlich auf standardisierte Verfahren zu verlassen.

Zum einen führen wir regelmäßig strukturierte Penetrationstests durch, die anhand definierter Prüfkategorien bewerten, ob öffentlich erreichbare Systeme oder Anwendungen potenzielle Verwundbarkeiten aufweisen. Diese Tests liefern uns ein systematisches und belastbares Bild über den aktuellen Sicherheitsstand unserer Systeme.

Darüber hinaus betreiben wir ein Bug-Bounty-Programm. Dabei wird unsere Plattform kontinuierlich von einer Vielzahl unabhängiger Sicherheitsforscher:innen geprüft, die mit unterschiedlichen Ansätzen und Fachperspektiven potenzielle Schwachstellen aufdecken, die in klassischen Tests nicht erfasst werden.

Ergänzend setzen wir automatisierte Analysetools ein, die laufend nach sicherheitsrelevanten Mustern und Abweichungen suchen und so unsere Angriffsfläche kontinuierlich überwachen.

Uns ist bewusst, dass sich Fehler nie vollständig ausschließen lassen. Durch die Kombination dieser Verfahren stellen wir jedoch sicher, potenziellen Angriffen frühzeitig begegnen zu können — sowohl durch strukturierte interne Prüfungen als auch durch den kontinuierlichen Einbezug externer Perspektiven.

Sicherheitsaudits für Lieferanten, Drittparteien und Unterauftragsverarbeiter

Für den Betrieb komplexer Systeme ist der Einsatz externer Unterauftragsverarbeiter (z. B. für Hosting und Betrieb) sowie weiterer Drittparteien, etwa Hersteller von Softwarekomponenten, Frameworks oder Bibliotheken, technisch notwendig. Diese Einbindung erfordert jedoch, dass wir uns auf das Sicherheitsniveau aller beteiligten Parteien uneingeschränkt verlassen können.

Unterauftragsverarbeiter im Sinne von Art. 28 DSGVO werden von der HASOMED GmbH vor ihrem Einsatz sorgfältig geprüft und in Auftragsverarbeitungsverträge eingebunden. Dazu gehören insbesondere die Bewertung ihres Informationssicherheitsniveaus, die Prüfung relevanter Zertifizierungen (z. B. ISO/IEC 27001, C5, SOC 2) sowie regelmäßige Audits im Rahmen unseres Informationssicherheits-Managementsystems (ISMS).

Wir begrenzen die Anzahl der eingesetzten Unterauftragsverarbeiter auf das notwendige Minimum und informieren unsere Kund:innen transparent über alle Änderungen. Eine stets aktuelle Liste aller Unterauftragsverarbeiter wird öffentlich zugänglich bereitgestellt.

Für sonstige Lieferanten und Drittparteien, bei denen keine Verarbeitung im Auftrag erfolgt (z. B. bei Softwarebibliotheken oder Hardwarelieferanten), führen wir strukturierte Due-Diligence-Prüfungen durch. Dabei betrachten wir nicht nur formale Nachweise, sondern auch organisatorische Aspekte, etwa:

- Welche Sicherheitsorganisation ist etabliert?
- Wie sehen die Prozesse im Bereich Incident Response oder Schwachstellenmanagement aus?
- Wie transparent kommunizieren die Anbieter über Schwachstellen oder Sicherheitsvorfälle?
- Entspricht das Gesamtbild den Anforderungen an eine belastbare Sicherheitskultur?

So stellen wir sicher, dass wir in der gesamten Lieferkette einen einheitlich hohen Maßstab anlegen — unabhängig davon, ob es sich um Auftragsverarbeiter oder sonstige Drittparteien handelt.

Strukturierte Incident-Response- und Kommunikationsabläufe

Auch bei bestmöglicher Vorbereitung lassen sich Sicherheitsvorfälle nie vollständig ausschließen. Entscheidend ist daher, wie schnell und koordiniert reagiert wird. Aus diesem Grund haben wir bei HASOMED klare Incident-Response-Prozesse etabliert, die technische Analyse, interne Koordination und externe Kommunikation systematisch miteinander verbinden.

Unsere Abläufe folgen definierten Schritten – von der ersten Erkennung über die Bewertung und Eindämmung bis hin zur nachhaltigen Behebung und Dokumentation. Dabei ist festgelegt, welche Rollen zu welchem Zeitpunkt eingebunden werden und wie die Eskalationswege verlaufen. Ein besonderer Schwerpunkt liegt auf der klaren Kommunikation: Sowohl intern zwischen den beteiligten Teams als auch extern gegenüber betroffenen Kund:innen und – falls erforderlich – gegenüber Aufsichtsbehörden.

Darüber hinaus betrachten wir auch sogenannte „near miss situations" – also Ereignisse, die potenziell kritisch hätten werden können, aber frühzeitig erkannt und

entschärft wurden. Diese Fälle fließen systematisch in unsere Lernprozesse ein. Unser Ziel ist nicht nur, Vorfälle effizient zu bearbeiten, sondern die Organisation dadurch langfristig stärker und resilienter zu machen.

Damit folgt unser Sicherheitsansatz dem Prinzip der Anti-Fragilität: Jede Störung oder Herausforderung ist für uns eine Gelegenheit, Strukturen und Abläufe zu verbessern. So entsteht ein System, das nicht nur widersteht, sondern sich kontinuierlich an neue Bedrohungen anpasst und daran wächst.

Für unsere Kund:innen bedeutet das: Im unwahrscheinlichen Fall eines Sicherheitsvorfalls können sie sich darauf verlassen, dass HASOMED schnell, strukturiert und offen reagiert – und dass jeder Vorfall zu noch mehr Stärke im Gesamtsystem führt.

4. Rechtliche Zulässigkeit & Compliance

Umgang mit (US-)Behördenanfragen

Die öffentliche Diskussion über mögliche Zugriffe ausländischer Behörden auf in der Cloud gespeicherte Daten – etwa im Kontext des **US CLOUD Act** – zeigt, wie wichtig technische und organisatorische Souveränität in Cloud-Architekturen ist. Der US CLOUD Act sieht vor, dass US-Behörden Cloud-Anbieter mit US-Eigentumsverhältnissen in bestimmten Fällen zur Herausgabe von Daten verpflichten können. Ein solcher Zugriff erfordert einen richterlichen Beschluss eines US-Bundesgerichts und kommt in der Praxis nur in sehr seltenen Ausnahmefällen vor. Gleichwohl berücksichtigen wir dieses Risiko in unserer Architektur und in unseren Prozessen ausdrücklich:

- RehaCom® Online wird **ausschließlich in zertifizierten Rechenzentren in Deutschland** betrieben. Patientendaten verlassen den deutschen Rechtsraum nicht.
- Sämtliche gespeicherten Daten sind **mit AES-256 verschlüsselt**, und der Zugriff auf das eingesetzte Schlüsselmaterial folgt einem strikten, rollenbasierten Berechtigungsmodell, das durchgängig protokolliert wird.
- **Anfragen ausländischer Behörden** ohne gültige deutsche oder europäische Rechtsgrundlage werden grundsätzlich abgelehnt.
- **Anfragen deutscher Behörden** werden durch die Geschäftsführung und unsere Rechtsabteilung sorgfältig geprüft, mit den zuständigen Aufsichtsbehörden abgestimmt und – sofern personenbezogene Daten betroffen sind – unter Einbeziehung der betroffenen Kund:innen bearbeitet.
- Soweit rechtlich zulässig, informieren wir betroffene Kund:innen über behördliche Zugriffe, damit sie eigene Widerspruchs- und Rechtsbehelfsmöglichkeiten wahrnehmen können.

So stellen wir sicher, dass ein behördlicher Zugriff ausschließlich auf Grundlage des geltenden deutschen und europäischen Rechts erfolgt und die Rechte unserer Kund:innen jederzeit gewahrt bleiben.

Zertifizierungen & Standards

Unsere Sicherheitsarchitektur und unsere organisatorischen Maßnahmen sind an etablierten internationalen Standards ausgerichtet und werden regelmäßig extern überprüft.

- Die **HASOMED GmbH** ist nach **ISO/IEC 27001** zertifiziert – dem international anerkannten Standard für Informationssicherheits-Managementsysteme (ISMS). Der Zertifizierungsumfang deckt ausdrücklich auch die Entwicklung und Bereitstellung webbasierter Softwarelösungen im Gesundheitswesen ab. Damit ist RehaCom® Online vollständig in das ISMS und seine Kontrollmechanismen eingebettet.
- RehaCom® Online wird zusätzlich nach dem **C5-Standard (Cloud Computing Compliance Criteria Catalogue)** des Bundesamts für Sicherheit in der Informationstechnik (BSI) testiert. C5 stellt sicher, dass Cloud-Dienste nach nachvollziehbaren, hohen Sicherheitskriterien betrieben werden.
- RehaCom® Online ist als **CE-zertifiziertes Medizinprodukt der Klasse I** gemäß der europäischen Medizinprodukte-Verordnung (MDR) konformitätsbewertet. Die zugrunde liegenden Qualitätsmanagementprozesse sind zudem in ein nach ISO 13485 geführtes QMS eingebettet.

Wir sehen uns verpflichtet, diese Zertifizierungen und Konformitätsbewertungen dauerhaft aufrechtzuerhalten und regelmäßig zu erneuern. Für unsere Kund:innen bedeutet das, dass unsere Sicherheitsmaßnahmen nicht nur intern definiert, sondern **durch unabhängige externe Prüfer bestätigt** sind.

DSGVO-Konformität

Die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) ist für uns selbstverständlich – sie bildet die rechtliche Grundlage für jede Verarbeitung personenbezogener Daten. Wichtig ist uns dabei, die Anforderungen der DSGVO nicht nur formal zu erfüllen, sondern „by design" in unsere Architektur und Prozesse einzubauen.

Zentrale Prinzipien wie Datenminimierung, Zweckbindung, Transparenz, Integrität, Vertraulichkeit und die Wahrung der Betroffenenrechte verstehen wir nicht nur als gesetzliche Vorgaben, sondern als praktische Leitlinien für unseren täglichen Umgang mit sensiblen Gesundheitsdaten.

Damit ist die DSGVO für uns mehr als ein regulatorischer Rahmen: Sie ist ein Gestaltungsprinzip, das wir konsequent in Technik, Organisation und Prozesse übersetzen.

5. Zusammenarbeit und Ausblick

Sicherheit ist für uns kein abgeschlossener Zustand, sondern eine gemeinsame Aufgabe, die sich ständig weiterentwickelt. Dieses White Paper soll deshalb nicht nur Einblick in unsere aktuellen Prinzipien und Maßnahmen geben, sondern auch zur Diskussion einladen.

Wir möchten offenlegen, wie wir Sicherheit bei HASOMED verstehen, und freuen uns über Rückmeldungen, Kritik und Anregungen. Denn wir sind überzeugt: Nur im konstruktiven Austausch mit unseren Nutzer:innen, Partner:innen und der Fachöffentlichkeit können wir unser Sicherheitsniveau kontinuierlich verbessern und gemeinsam eine verlässliche digitale Versorgung in der Neurorehabilitation gestalten.