PRIVACY AND SECURITY INFORMATION

INTRODUCTION

This document outlines the privacy and security implications related to the ICHOM Global Benchmarking Platform. It is intended for privacy and security officers or other people who want to be informed about our privacy and security measures. Others, like IT managers, quality offers, may also be interested.

MRDM has been selected as the data processor for the ICHOM project. As a qualified, specialized and dedicated data processor, MRDM focuses on benchmarking health outcomes. MRDM helps healthcare providers worldwide to collect, validate and compare data efficiently and scale using quality assured ICHOM Sets of Patient-Centered Outcome Measures.

MRDM is a trusted partner in medical data. Therefore, privacy and security are core elements in all activities. MRDM is ISO27001 certified and complies to General Data Protection Regulation (GDPR) (European Economic Area) and Health Insurance Portability and Accountability Act (HIPAA) (USA) privacy regulations. MRDM mainly acts as a data processor for healthcare institutions. MRDM is a company that processes personal data in the context of activities of its establishment in the EU.

PRIVACY AND SECURITY IMPLICATIONS

Data Processor Agreement (GDPR) / Business associate agreement (HIPAA)

Before MRDM can deliver their services, the required legal documentation, such as a Data Processor Agreement, (GDPR) or Business Associate Agreement (HIPAA) needs to be put in place. These documents detail the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of MRDM as a processor and allow MRDM to work with personal data concerning health on behalf of the data controller. The controller (GDPR) or the covered entity (HIPAA) is the healthcare institution.

Access and security

Access to various parts of the infrastructure of the benchmarking platform depends on the user's authorization level. The authorization and authentication method is linked to personal accounts with two-factor authentication. MRDM specifically puts effort into ensuring the user's identity in relation to his or her organization.

MRDM collects, pseudonymizes, aggregates and encrypts data. Data is encrypted at all times during transport (encrypted in transit) and storage (encrypted at rest). The encryption of data and traffic is designed in accordance with the best practices as identified by the Dutch National Cyber Security Center and international institutes like the National Institute of Standards and Technology (ENISA/NIST).

Furthermore, incidents are proactively managed, penetration-tests are performed and the security of the data continuously monitored. For example, unauthorized access attempts are registered and analyzed. For back-up purposes, data is stored redundantly and separately from the production environment. The key goal for back-ups is to provide disaster recovery, losing a minimal amount of data in the event of a disaster, while making sure systems are quickly back up and running.

Finally, data is only shared with agreed upon parties and in accordance with existing contracts. Third parties and suppliers are screened at all times and questioned on fixed subjects. That guarantees a level of security and privacy that is at least comparable to the standards of MRDM. Suppliers and third parties are explicitly asked to demonstrably mitigate specific risks. The suppliers and third parties are regularly monitored based on MRDMs demands for collaboration.

Infrastructure

MRDM uses cloud providers (subcontractors) for the processing of customer data. MRDM makes agreements with clients and subcontractors about the regions in which the processing of customer data may take place. The default region is the Netherlands (EEA).

MRDM concludes agreements with its subcontractors that comply with all applicable privacy legislation and security standards. All customer data services are completely separate from MRDM's corporate data services.

When the default option is not legally allowed in your geography, decentralized hosting will also be available. In this way, data will not leave your country. The estimation is that in 2022 we will also offer decentralized hosting in another nationally accepted cloud provider, and from 2023 local cloud hosting.

People

MRDMs privacy and information security office designs, implements and oversees secure work processes. Its staff is trained in accordance with industry standards (CIPP/E, CIPM and CIPT). Furthermore, staff are asked to submit certificates of conduct and are obliged to secrecy by signing an NDA.

MRDM deploys security and privacy by design, which means that both aspects are integrated into the design of a product or service. All steps in the data handling process are taken into account.

To additionally ascertain full compliance with all relevant legislation regarding privacy, data security and other relevant issues, MRDM cooperates closely with law firms specializing in European and international privacy regulations, with a specific focus on the healthcare sector.

Data deliveries to ICHOM or third parties

Customer data processed by MRDM is never shared with ICHOM or third parties unless this has been agreed in agreements between ICHOM and the Customer or between the Customer and MRDM.