MOLECULAR HEALTH

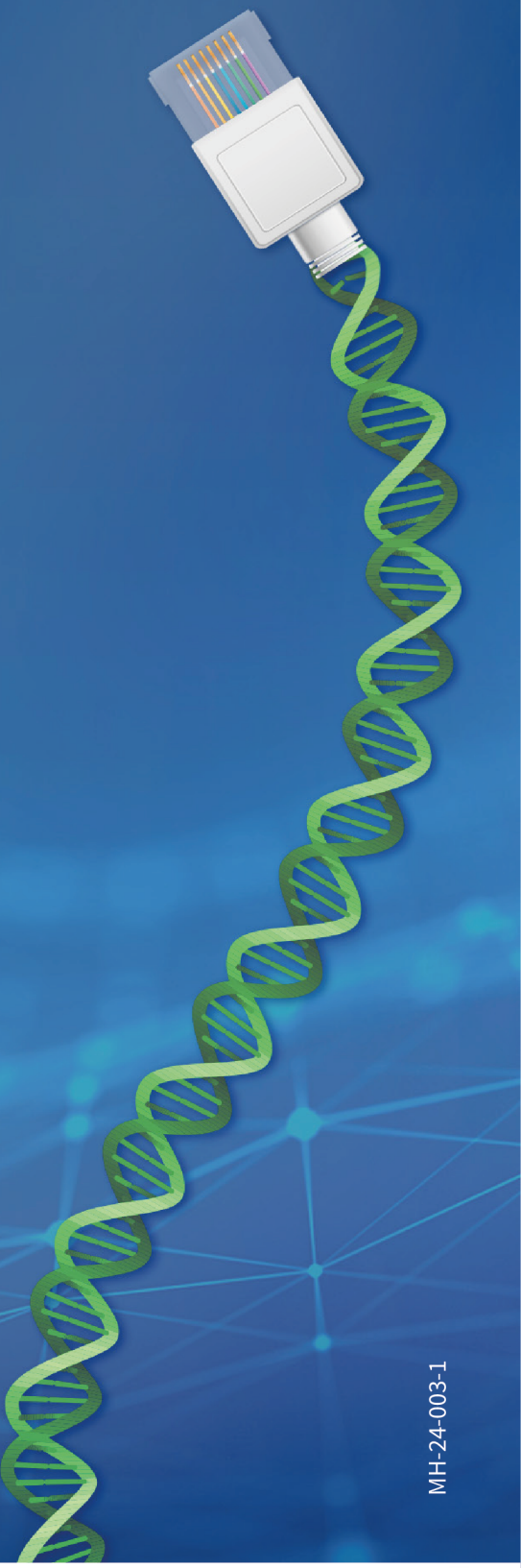
Better data. Better insights.
Better outcomes.
molecularhealth.com

GUIDE

Data security and Data privacy by design

Your sensitive data is safe with us

IVDR
(EU) 2017/746



MH-24-003-1

MH Guide product description:

MH Guide is a stand-alone software as a service (SaaS) used for in vitro examination of next-generation sequencing (NGS) data or genetic and molecular alteration data. MH Guide provides critical insights to aid in the determination of treatment options and translates genomic data into actionable cancer treatment strategies based on genetic biomarkers and medical guidelines for patients diagnosed with cancer (solid and hematological tumors). MH Guide enables laboratories and medical professionals to enhance and scale-up their molecular testing workflows in oncology. MH Guide is an in vitro diagnostic software CE marked in Europe under (EU) 2017/746 (IVDR).

MH Guide/BRCA provides information to determine hereditary cancer predisposition for patients suspected of being at risk of a hereditary predisposition to breast and ovarian cancer syndrome (HBOC). MH Guide/Mendel provides information to aid in the diagnosis of hereditary diseases or disease predispositions for patients suspected of being at risk of these diseases.

MH Guide and its modules MH Guide/BRCA and MH Guide/Mendel are used as expert systems for patient management by trained healthcare professionals qualified in genetics, oncology, and molecular diagnostics.

Pivotal Data Security features with MH Guide

Data Center, Transparency, and Guaranteed data residency

MH Guide is hosted in data centers that comply with latest security standards, such as ISO 27001 and Trusted Site Infrastructure (TSI). Molecular Health is committed to adhering to regional and global security policies to ensure seamless implementation of software services for MH Guide customers. Also, MH Guide complies with data residency and privacy requirements to address local regulatory requirements and support customers operating in a regulated environment.

Availability

MH Guide is hosted in data centers that comply with security standards, including ISO 27001 and In the context of cloud computing services, there are internal and external availability risks. To address these concerns, Molecular Health has integrated a business continuity and disaster recovery plan into its business processes. MH Guide is installed on a high- availability cloud infrastructure that adheres to Uptime Institute Tier III design standards and ISO 27001 to ensure dedicated network connectivity, redundancy, uninterruptible power supply (UPS), and effective data backup strategies.

Record keeping and audit logs

MH Guide enables record keeping and audit logging, ensuring full traceability for all objects and actions carried out in the system.

Independent Third-Party Penetration Tests

Molecular Health regularly performs external third-party penetration testing for MH Guide and maintains a continuous process for vulnerability scanning and handling.

Encryption for sensitive data

MH Guide prioritizes confidentiality of data processing activities in the cloud environment. Data uploads to MH Guide and usage of the application use secure (SSL) protocols and transfer layer security (TLS 1.2 or higher). PHI data are encrypted on the customer side to ensure the highest level of security.

Data Isolation

MH Guide offers the highest degree of data isolation by implementing industry-standard data segregation techniques, including the need-to-know principle, enforced through technical and organizational measures, e.g., role-based access governed by fine-grained security controls.

Data management and retention

MH Guide stores customer data to protect against data loss. All necessary information and files are stored in compliance with applicable federal and state regulations.

Integrity

MH Guide uses public key infrastructure (PKI); hashing techniques ensure data flow integrity and origination across the entire solution. Frequent customer database backup is performed to decrease the risk of data loss. In addition, the system contains logging that provides notification when data are altered. If improper alteration is detected, rolling back to a previous backed up version is available.

Login policies

MH Guide enforces strong password requirements, a renewal period, and inactivity timeout. Individualized logins are also available, enabling multiple users to utilize the platform per instance.

Role-based management of sensitive data

MH Guide supports customers operating in regulated environments with stringent compliance requirements. MH Guide includes fine-grained, configurable access controls that govern individual user access and management of sensitive PHI/PII data within the platform. To prevent error, data loss, or tampering, system access is restricted based on which roles require access and the tasks those roles are required to complete.

Shared responsibilities

Molecular Health is responsible for protecting the infrastructure that runs all of the Software as a Service. This infrastructure is composed of the hardware, software, networking, and facilities that run MH Guide services. Part of this responsibility requires that Molecular Health performs recurring security patch updates or other updates to protect the environment from emerging threats and supports iterative improvements. Customers required to comply with HIPAA are responsible for ensuring that they have a HIPAA compliance program in place and that they use MH Guide in a manner to ensure their compliance.

Firewall & Cybersecurity Monitoring

MH Guide is secured by a state-of-the-art web application firewall and is subject to continuous cybersecurity monitoring.

Pivotal Data Protection features with MH Guide

Privacy by design

MH Guide supports customers operating in regulated environments and is in accordance with current data protection laws, including GDPR, HIPAA, and German Genetic Diagnostics Act (GenDG). The Molecular Health facilities that process protected health information (PHI) or personally identifiable information (PII) are in compliance with HIPAA and employ industry best practices such as:

- Buildings are monitored 24 hours a day and keycard accessed
- Offices have a monitored security system
- Any access to IT-Infrastructure from outside the office is via a secure Virtual Private Network (VPN)
- PHI data are transferred and stored encrypted and are protected by additional authentication mechanisms

Conformity	Description
ISO 27001 Trusted Site Infrastructure (TSI)	Data centers employed for the hosting of MH Guide are selected based on existing TSI and/or ISO 27001 certification
ISO 14971	Application of risk management to medical devices
EN ISO 13485	Medical devices – Quality management systems – Requirements for regulatory purposes. Molecular Health is certified according ISO 13485 for the scope "Design, Development and Manufacture of software systems for the integrated analysis of clinical and genomic patient data to support treatment decisions and provision of related services"
IEC 62304	Medical device software – Software life cycle processes
(EU) 2017/746	European Regulation on in vitro diagnostic medical devices (IVDR)
CLIA/CAP	Molecular Health is certified according to the quality standards of the US Clinical Laboratory Improvement Amendments (CLIA), which are issued by the US federal agency Centers for Medicare and Medicaid Services (CMS). Molecular Health is accredited by the College of American Patho-logists (CAP), and thus complies with US laboratory standards to ensure proper validity, handling, and reporting of dry-lab results
MDSAP	Molecular Health is a certified Medical Device Single Audit Program (MDSAP) company with the scope: "Design and Development, Manu- facture, Installation and Servicing of In-Vitro Diagnostic Software used in Genetic Testing for Diagnosis of Hereditary Diseases or Predispositions to a Medical Condition or a Disease and Prediction of Treatment Response including Point of Care In-Vitro Diagnostic Medical Devices"