MH GUIDE
MH GUIDE CAS

Data security and Data privacy by design

Your sensitive data is safe with us

MH-24-003-2

©2025 Molecular Health GmbH. All rights reserved.

MH Guide and MH Guide CAS product descriptions:

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.

MH Guide Case Annotation Solution (MH Guide CAS) is a software for research labs to annotate genetic and molecular alteration data from a tumor specimen with published therapy associations, biomarkers, and recruiting clinical trials. MH Guide CAS is for Research Use Only. Not for diagnostic procedures.

Robust data security features with MH Guide and MH Guide CAS

Secure, certified, and transparent data hosting

Security and privacy are core pillars of the MH Guide platform – embedded into every layer of its design, deployment, and operation. MH Guide and MH Guide CAS are hosted in data centers and with providers certified to internationally recognized security standards, including Trusted Site Infrastructure (TSI), and ISO 27001 – demonstrating our commitment to best-in-class data protection and operational excellence.

Molecular Health ensures compliance with regional and global security frameworks to support the reliable and compliant deployment of its software services.

Key data center and hosting security features include:

- Compliance with data residency, privacy, and sovereignty requirements, allowing customers to retain full control over sensitive data
- Certified infrastructure that meets international security and audit standards
- Advanced encryption protocols (SSL/TLS, AES-256) to safeguard data in transit and at rest
- Full adherence to local and international regulations, including the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and the German Genetic Diagnostics Act (GenDG).

These comprehensive measures ensure that MH Guide provides a secure, privacy-compliant environment for all users handling with sensitive data.

Data residency – regional hosting with certified security

MH Guide and MH Guide CAS ensure that your data are securely processed and stored in region-specific data centers operated by certified hosting providers. All hosting environments meet internationally recognized security standards, including Trusted Site Infrastructure (TSI) and ISO 27001 certifications –supporting compliance, data sovereignty, and customer trust.

Regional Hosting Locations:

- Heidelberg iT located in Heidelberg, Germany
- AWS Europe located in Paris (Region eu-west-3), offering HDS-certified (Hébergeur de Données de Santé) service for France, and ACN-qualified (Agenzia per la Cybersicurezza Nazionale) service for Italy
- AWS U.S. located in Ohio (Region us-east-2) from which MH Guide CAS is hosted for the US market Both MH Guide CAS and AWS are certified under TX-RAMP (Texas Risk and Authorization Management Program), meeting stringent state-level cybersecurity and data protection requirements.

Molecular Health's commitment to data residency empowers customers to maintain control over where their data is stored – supporting local compliance, minimizing cross-border risks, and ensuring privacy-by-design across all deployments.

Availability

MH Guide and MH Guide CAS are deployed on high-availability cloud infrastructures that comply with Uptime Institute Tier III design standards. This infrastructure includes:

- Redundant systems for network connectivity and power supply (UPS)
- Reliable data backup strategies to prevent data loss
- Dedicated infrastructure to ensure consistent performance and uptime

Molecular Health also maintains a business continuity and disaster recovery plan to minimize the impact of potential internal or external disruptions. These measures help ensure that MH Guide and MH Guide CAS remain consistently available and resilient against service interruptions.

Record keeping and audit logs

MH Guide and MH Guide CAS provide comprehensive record keeping and audit logging, ensuring full traceability of all objects, actions, and user activities within the system. This allows organizations to meet compliance requirements, support internal reviews, and maintain transparency across all processes.

Independent Third-Party Penetration tests

Molecular Health conducts regular third-party penetration tests on MH Guide and MH Guide CAS to identify and address potential security vulnerabilities. These independent assessments are complemented by a continuous internal process for vulnerability scanning and remediation, ensuring the platform remains secure and up to date with evolving cybersecurity threats.

Encryption for sensitive data

MH Guide and MH Guide CAS ensure the highest level of data confidentiality in the cloud. All data uploads and application usage are protected with industry-standard Secure Sockets Layer (SSL) protocols and Transport Layer Security (TLS 1.2 or higher). To further safeguard protected health information (PHI)[1], data is encrypted on the customer side before transmission – ensuring maximum security and compliance from the outset.

Data isolation and role-based management of sensitive data

MH Guide and MH Guide CAS ensure a high level of data isolation through industry-standard data segregation techniques, with access governed by the need-to-know principle. Both technical and organizational measures enforce role-based access control (RBAC), supported by fine-grained, configurable security policies that limit data visibility and permissible actions per user role. This minimizes the risk of errors, data loss, or unauthorized changes, ensuring that sensitive information is handled exclusively by authorized personnel in compliance with internal policies and external regulations.

Additionally, MH Guide is designed for customers in highly regulated environments, the platform restricts access to sensitive data – such as protected health information (PHI) and personally identifiable information (PII) – so that each user can only access and manage the data and functions necessary for their specific responsibilities.

Reliable data management

MH Guide and MH Guide CAS securely store customer data to ensure protection against loss and maintain continuity. All data is retained in full compliance with applicable federal and state regulations, providing peace of mind and regulatory assurance.

Data integrity

MH Guide and MH Guide CAS ensure end-to-end data integrity using public key infrastructure (PKI) and hashing techniques, which verify both the authenticity and consistency of data throughout the platform.

To further protect against data loss or unauthorized changes, MH Guide and MH Guide CAS include:

- Frequent customer database backups
- Audit logging and alerts for any data modifications
- The ability to roll back to a previous backup version if unauthorized or improper changes are detected

These measures provide strong safeguards to maintain the accuracy, reliability, and traceability of all data within the system.

Login policies

MH Guide and MH Guide CAS enforce strict login and password policies to ensure secure access to the platform. These include:

- Strong password requirements to enhance account protection
- An automatic session timeout after periods of inactivity to prevent unauthorized access

In addition, MH Guide and MH Guide CAS support individualized user logins, allowing multiple users to access the platform securely within the same instance, while maintaining user-specific activity tracking and access controls.

Data retention and deletion aligned with regulatory standards

Customer data retention and deletion is following the applicable statutory requirements such as the General Data Protection Regulation (GDPR) or German Genetic Diagnostics Act (GenDG). After mandatory retention periods, data can be deleted from our servers upon request or through a predefined deletion routine – ensuring compliance and customer control over data lifecycle management.

Shared responsibilities for security and compliance

At Molecular Health, we take responsibility for securing the infrastructure that powers MH Guide and MH Guide CAS – including hardware or Platform as a Service (PaaS), software, networking, and facilities behind our Software as a Service (SaaS). As part of our ongoing commitment, we perform regular security patches and updates to defend against emerging threats and support continuous improvement of our platform.

Customers subject to HIPAA regulations are responsible for implementing their own HIPAA compliance programs and for using MH Guide CAS in a manner that supports their compliance obligations.

Advanced firewall protection and continuous cybersecurity monitoring

MH Guide and MH Guide CAS are protected by an integrated cutting-edge security infrastructure, including firewalls, web application firewalls, and system- and security monitoring systems. This combination ensures multi-layered defense against cyber threats: real-time detection and blocking of malicious traffic, protection of web applications against OWASP Top 10 vulnerabilities (Open Worldwide Application Security Project), and continuous security analytics for proactive threat identification. With 24/7 monitoring and automated threat response, we provide our customers with robust, enterprise-grade protection.

GDPR compliant

HIPAA compliant

Robust data protection features with MH Guide and MH Guide CAS

Privacy by design

MH Guide and MH Guide CAS are designed to support customers operating in highly regulated environments, ensuring compliance with key data protection regulations including General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and the German Genetic Diagnostics Act (GenDG). Our commitment to safeguarding sensitive data is backed by rigorous protocols and industry best practices.

Molecular Health facilities that process protected health information (PHI)[1] or personally identifiable information (PII) are fully HIPAA-compliant and incorporate advanced security measures, including:

- 24/7 monitored buildings with controlled keycard access
- Secure, monitored office environments
- Remote access restricted to a secure Virtual Private Network (VPN)
- End-to-end encryption of PHI data during transfer and storage, protected by robust authentication mechanisms

With MH Guide and MH Guide CAS, your data are protected by a security-first infrastructure built for trust and compliance.

Conformity	Description
ISO 27001 Trusted Site Infrastructure (TSI)	Data centers and hosting providers employed 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 to ISO 13485 for the scope“ Design, Development and Manufacture of in-vitro-diagnostic software systems for molecular and genetic testing based on data from Next Generation Sequencing or other technologies to support patient management decisions for constitutional diseases, or cancer 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 Pathologists (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, Manufacture, 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“

MH Guide is offered by Molecular Health’s global strategic partner Integrated DNA Technologies (IDT) in the EU and European Free Trade Association (EFTA) States where IVDR applies, e.g., Switzerland.

MH Guide Case Annotation Solution (MH Guide CAS) is offered by Molecular Health’s global strategic partner Integrated DNA Technologies (IDT) in the U.S., and non-EU, or non-EFTA (European Free Trade Association) countries.

[1] PHI is not supported in the standard configuration of MH Guide CAS.