

Data Privacy & Security



Roche considers security and privacy of customer data a priority. We apply strict measures and controls to protect the data of healthcare institutions and their patients.

Secure storage

All medical and personal data is stored securely in ISO 27001 compliant data centres. **The infrastructure is HITRUST certified and it is on the Amazon Web Services Cloud** which includes **physical security measures** such as fencing, walls, security staff, video surveillance, intrusion detection, access control systems, etc., and **digital security measures** such as ID authentication, automatic blocking/locking mechanisms, data encryption, multiple authorization levels, minimum passwords requirements, VPN connections, etc., **based on Roche security standards**. A logging system is in place to ensure that **the actions performed are traceable** and that the audit trails are kept.

Continuous security process

Roche has implemented a multidimensional defence strategy for enhanced data protection and management.

- › **Privacy by Design:** Prominent data-protection principles, such as data minimisation and encryption of data are followed as Roche is committed to continuously maintain and enhance data security and privacy.
- › **Privacy by Default:** Only necessary personal data as per a specific purpose is processed and it involves the amount of personal data collected, the extent of the respective processing and the period of its storage and accessibility.
- › **Availability Control:** All data is protected against accidental and/or unauthorised destruction as appropriate backup processes and respective business contingency plans are in place.
- › **Third Party Management:** Roche executes strict controls while selecting external service providers and ensures that proper contractual arrangements and supervisory follow-up checks are in place.



Vulnerability management

Continuous monitoring and threat analysis procedures, for countering new vulnerabilities and security threats for the RocheDiabetes Care Platform. These include:

- › **Proactive Data Protection:** Internal and external penetration tests and corresponding assessments and evaluations are regularly performed.
- › **Incident Response Management:** Roche applications and underlying infrastructure is constantly monitored, to detect security events or potential incidents.
- › **Patch Management:** Security patch management is implemented to provide regular and periodic deployment of relevant security updates.

Secure transmissions

- › **Data Transfer Control:** All data communications for the RocheDiabetes Care Platform via Internet are secured by using SSL over the HTTP protocol. Roche credentials and access rights are required to be able to connect through VPN connections.
- › **Data Entry Control:** Roche has implemented a logging system for input, modification and deletion of data. Authorisation controls are also in place, so the validation verifies that each logged in user is entitled to perform an action in the system.

Pseudonymization and encryption

All collected clinical medical data are properly pseudonymized, encrypted and stored in a separate database than the specific Data Subject Identifiable Data. Clinical and non-clinical databases are linked to each user through an individually assigned ID.

Fostering faster connections



For more information
RocheDiabetes.com/CarePlatform

© 2020 Roche Diabetes Care

Roche Diabetes Care GmbH
Sandhofer Str. 116
68305 Mannheim