cobas e 411 analyzer

Addendum 2 to Safety Manual V1.2
Software version 03-01

Publication information

Publication version	Software version	Revision date	Change description
1.0	03-01	2020-04	Section on the General Data Protection Regulation (GDPR) has been added to the Safety Manual version 1.2 (2019-02).

▦ Revision history

Edition notice

This addendum contains supplementary information for users of the **cobas e** 411 analyzer.

Copyright

Trademarks

The following trademarks are acknowledged:

COBAS, COBAS C, COBAS E, and ELECSYS are trademarks of Roche.

All other trademarks are the property of their respective owners.

Contact addresses

Inside the European Union and EFTA member states

🏭

Manufacturer of **cobas e** 411 instrument

Hitachi High-Technologies Corporation
1-24-14 Nishi-Shimbashi
Minato-ku Tokyo 105-8717
Japan

EC REP

Authorized representative

Roche Diagnostics GmbH
Sandhofer Strasse 116
68305 Mannheim
Germany

Outside the European Union and EFTA member states

Manufactured by:

Hitachi High-Technologies Corporation

Manufactured for:

Roche Diagnostics GmbH
Sandhofer Strasse 116
68305 Mannheim
Germany

Revision 1: Safety precautions

The following topic on the General Data Protection Regulation (GDPR) has been added to the Safety Manual.

The new topic provides additional information and consolidates information that was previously contained in other sections of the Safety Manual.

The following section of the Safety Manual is omitted because the information was consolidated:

- Caution messages > Data security

In this section

About the protection of personal data and software security (3)

About the protection of personal data and software security

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all citizens of the European Union (EU) and the European Economic Area (EEA). The regulation also covers the processing of personal data outside the EU and EEA areas.

If this regulation or any other privacy protection regulation is applicable for your country, observe the following safety messages to prevent data breaches and to meet the GDPR:

Access control

Unauthorized access may lead to data breaches.

- Implement physical access controls to ensure that only authorized laboratory staff operate the system at all times.
- Assign a personal, unique user ID to each user for system access.
- Assign access rights to each user only as high as required for the tasks of the user.
- Delete user IDs from the system for users who no longer work on the system.

Corrupt data due to a disclosed password

The security of the system and its data depends on the password-protected access. If an unauthorized person discovers your user ID and password, they could compromise this security.

- Always enter your password unobserved.
- Do not write down your password anywhere, including in a contact form, in the address book, or in a file on the computer.
- Do not disclose your password to anyone. Roche will never ask you for your password.
- If you ever disclose your password to anyone, change it immediately afterwards.
- Contact your local Roche affiliate if you think your account has been compromised.

Network security

Malicious software and hacker attacks may impair IT security. The laboratory is responsible for the IT security of their IT infrastructure.

- To protect and separate Roche systems from other laboratory infrastructure, the Roche-provided firewall must be used.
- Secure all devices and services used in the lab infrastructure against malicious software and unauthorized access.
- Secure the network environment to be resilient against traffic redirection and eavesdropping.

Data entry and data transfer

Writing patient sensitive information in comment fields can violate protection laws for protected health information.

- Do not write any patient sensitive information into comment fields.
- Do not download patient identifiers from any host system (e.g., LIS, middleware, or HIS) onto the system. Data transfer using any host protocol (e.g., ASTM) is not encrypted; data is transferred as plain text and readable with IT tools like sniffer.

Secure data storage

Unauthorized access to data backups and archive files can violate data protection laws.

- Any data backup or data archive that has been exported from the instrument must be physically stored in a secured location.
- Ensure only authorized persons may access the secure data storage. This includes the data transfer to remote storage locations and disaster recovery.
- Data backups must not be taken from the secure data storage. Do not take external storage devices outside the laboratory environment.

Cybersecurity and privacy awareness

Insufficiently informed employees can endanger security.

- Perform regular cybersecurity and privacy awareness trainings for laboratory staff handling personal data. Instruct laboratory staff how to handle data in a compliant way and according the privacy principles as mandated by customer regulations.
- Check your instrument for suspicious activity and report any suspected compromise to your local Roche representative immediately.
- Update to the latest software versions provided by Roche as soon as possible.
- Do not use external storage devices or storage media (e.g., USB flash drives or DVDs) on the system that have been used on public or private computers. Failure to do so may result in data loss and render the instrument unusable.

Use of storage media

Wrong handling of storage media may result in data loss or system malfunction.

- Insert or remove a DVD only when the instrument is in **Standby** mode.
- Do not use DVDs with low quality or damage (e.g., scratches, dirt, or dust on disks).
- At any one time only one storage medium can be in use. Before inserting a USB flash drive into a USB port, check that no other USB flash drive is connected and no DVD is inserted.
- Before removing a USB flash drive, safely disconnect it from the system using the corresponding button.

Computer viruses

If you detect an unexpected operation or program/data damage, the PC may be infected with a computer virus.

- To avoid virus infections, scan removable storage media by an antivirus software before using them on the system.
- Never use a program or storage medium that is suspected of containing a virus.
- If you think your PC is infected with a computer virus, call your local Roche Service representative. Your local Roche Service representative will check your system for proper functionality.

Data backup

Data may get lost due to hard disk failures or damages.

- Back up your data (measurement results and system parameters) at regular intervals.
- Use the backup function daily to store relevant data on the hard disk.
- Make a backup copy if you have changed any system parameters.

Non-approved third-party software

Installation of any third-party software that is not approved by Roche Diagnostics may result in incorrect behavior by the system.

- Do not copy or install any software or software patches on the system unless it is part of the system software or your Roche Service representative advises it.
- Do not change any PC settings.