cobas® 8000 modular analyzer series

Addendum 1.0 to Operator's Manual and Safety Guide version 5.4
Software version 06-07

Roche

cobas®

Life needs answers

Publication information

Publication version	Software version	Revision date	Change description
1.0	06–07	2020-03	Safety Guide: Section on the General Data Protection Regulation (GDPR) added. Operator's Manual: Specifications of sample barcodes revised

⊞ Revision history

Edition notice

This addendum contains supplementary information for operators of the **cobas**® 8000 modular analyzer series. It is meant to complement Version 5.4 of the Safety Guide and Operator's Manual.

Copyright

© 2007–2020, Roche Diagnostics GmbH.
All rights reserved.

Trademarks

The following trademarks are acknowledged:

COBAS, COBAS C, COBAS E, COBAS INTEGRA, and LIFE NEEDS ANSWERS are trademarks of Roche.

All other trademarks are the property of their respective owners.

Approvals

The **cobas**® 8000 modular analyzer series meets the requirements laid down in:

Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices.

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.
To view the full text of the 2014/53/EU declaration of conformity, go to the Roche DiaLog Global Web Site (*https://dialog1.roche.com/*) and choose the eLabDoc link.
If you are unable to access Roche DiaLog, contact a Roche Service representative.

The full text of the 2014/53/EU declaration of conformity is available at the following internet address: http://e-labdoc.roche.com

Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Compliance is provided by means of the Declaration of Conformity.

The following marks demonstrate compliance:

IVD For *in vitro* diagnostic use.

$\mathrm{C}\,\mathrm{E}$ Complies with the IVD directive 98/79/EC on *in vitro* diagnostic medical devices

Issued by Intertek for Canada and the US.

Contact addresses

Inside the European Union and EFTA member states

	Manufacturer of the instrument	Hitachi High-Technologies Corporation 1-24-14 Nishi-Shimbashi Minato-ku Tokyo 105-8717 Japan
	Manufacturer of **cobas**® 8000 data manager	Roche Diagnostics GmbH Sandhofer Strasse 116 D-68305 Mannheim Germany
EC REP	Authorized representative	Roche Diagnostics GmbH Sandhofer Strasse 116 D-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

Table of contents

Revision 1: Safety precautions

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

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

The following sections of the Safety Guide are omitted because the information was consolidated:

- Caution messages > Software and data security
- Notices > Data security

In this section

About the protection of personal data and software security (5)

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., HL7, 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 storage media outside the lab 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.

‣ Do not connect external storage devices to the USB ports on the system, unless instructed to by the user documentation or by a Roche Service representative.

Use of storage media

Incorrect 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 low quality or damaged DVDs (e.g., scratches, dirt, or dust on disks).

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.

Revision 2: Specifications of sample barcodes

The ISBT 128 standard has been added to the list of supported barcode types for the identification of blood donations.

In this section

Specifications of sample barcodes

	Specifications	
Supported barcode types	Codabar (Japan: NW-7)	
	Code 39	
	Interleaved 2 of 5 (ITF)	
	Code 128 (including the ISBT 128 Donation Identification Number)	
Check digit	All barcode types must be used with a check digit	
Number of digits for IDs	Codabar (NW-7)	6 digits + 1 check digit
	Code 39	3–22 digits + 1 check digit
	Interleaved 2 of 5	3–21 digits + 1 check digit
	Code 128 (including the ISBT 128 Donation Identification Number)	4–22 digits + 2 check digits
Permitted characters	Codabar (NW-7)	0 to 9, -, /, ., $, :, +
	Code 39	0 to 9, A to Z, -, ., [ ], /, +, $, %
	Interleaved 2 of 5	0 to 9
	Code 128 (including the ISBT 128 Donation Identification Number)	ASCII characters (128 characters)
Check digit calculation algorithm	Codabar (NW-7)	Modulus 16
		Modulus 11
		Modulus 10/2 Weight
		Modulus 10/3 Weight
		7 Check DR
		Weight Modulus 11
		Modulus 10/2 Weight-A
	Code 39	Modulus 43
	Interleaved 2 of 5	Modulus 10/3 Weight
	Code 128 (including the ISBT 128 Donation Identification Number)	Modulus 103
Barcode quiet zone at both ends of barcode image	≥ 5 mm	

⊞ Specifications of sample barcodes