Addendum 1.0

to Operator´s Manual Version 8.2
***cobas**® 6000 analyzer series*
Software Versions 06–03

Document information

Revision history

Document version	Software version	Revision date	Changes
Addendum 1.0 to Operator’s Manual Version 8.2	06-03[a][b][c]	November 2019	

(a) Also valid for software version 05-02

(b) Also valid for software version 06-01

(c) Also valid for software version 06-02

Edition notice

This addendum contains supplementary information for operators of the **cobas** 6000 analyzer series. It is meant to complement the Operator´s Manual Version 8.2.

Every effort has been made to ensure that all the information is correct at the time of publishing. However, Roche Diagnostics reserves the right to make any changes necessary without notice as part of ongoing product development.

Copyright

Changes to the Operator´s Manual Version 8.2

This addendum includes additional information for the chapter *General safety information* of the Operator's Manual Version 8.2.

The following information are changed or added:

- Additional information for *Safety precautions* > *Safe and proper use of the instrument*
  - ◦ Personal injury and infection due to sharps, rough edges, and/or moving parts
- Changed information for *Safety precautions* > *Safe and proper use of the instrument* > *Biohazardous materials*
  - ◦ Waste
- Additional information for *Software and data security* about the General Data Protection Regulation (GDPR).
  - ◦ Protection of personal data and software security

Safe and proper use of the instrument

Personal injury and infection due to sharps, rough edges, and/or moving parts

Good Laboratory Practice can reduce the risk of injury. Be aware of your laboratory environment, well-prepared, and follow the instructions for use.
Some areas of the instrument may have sharps, rough edges, and/or moving parts.

- Wear personal protective equipment to minimize the risk of injury from bodily contact with such parts, especially in less accessible areas, or while cleaning the instrument.
- Your personal protective equipment should be appropriate to the degree and type of potential hazard, e.g. suitable lab gloves, eye protection, lab coat, and footwear.

Biohazardous materials

Waste

Contact with liquid waste may result in infection. All materials and mechanical components associated with the waste systems are potentially biohazardous.

- Wear appropriate protective equipment.

  👁 See *Personal protective equipment* on page A-9.
- If any biohazardous material is spilled, wipe it up immediately and apply disinfectant.
- If liquid waste comes into contact with your skin, wash it off immediately with water and apply a disinfectant. Consult a physician.

Waste must be treated in accordance with the relevant laws and regulations. Any substances contained in reagents, calibrators, and quality controls, which are legally regulated for environmental protection, must be disposed of according to the relevant water discharge facility regulations.

Two kinds of liquid waste are discharged by the instrument:

- Concentrated liquid waste that contains highly concentrated reaction solution. Treat this waste as infectious waste. Dispose of this waste according to the appropriate local regulations.
- Dilute waste: A non-concentrated liquid waste diluted with rinsing water from cell wash or water from the incubator bath. When using NaOH-D for washing the reaction cells, alkaline concentration is 0.1 to 1.0 mmol/L in terms of sodium

hydroxide equivalence. Dilute waste is discarded through tubes at the rear of the instrument.

When disposing of any waste generated by the instrument, do so according to the relevant laws and local regulations.

Liquid waste and replacement parts such as reaction cells and ISE electrodes have to be treated as infectious medical waste.

👁 For information on disposal of the instrument, see *Disposal of the instrument* on page A-33.

Protection of personal data and software security

The General Data Protection Regulation (GDPR) is a regulation 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 these laws or any other privacy protection regulations are applicable for your country, observe the following safety messages to prevent data protection breaches and to meet the GDPR:

Access control

Unauthorized access may lead to data protection breaches.

- Implement physical access controls to ensure that only authorized personnel operate the system at all times.
- Assign a personal, unique operator 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 operator 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 lab 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 patient 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 external storage devices outside the lab environment.

Cyber security and privacy awareness

Insufficiently informed employees can endanger security.

- Perform regular security and privacy awareness trainings for staff handling personal data. Instruct 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.
- Exercise care when you use storage media such as DVDs. Do not connect to the system any storage media that you use on public or home computers. Failure to do so may result in data loss and render the instrument unusable.

USB storage devices

USB storage devices can be used for several kinds of data backups and restores. Wrong handling of a USB storage device may result in data loss or malfunction of the instrument.

- Insert or remove a USB storage device only when the instrument is in standby mode.
- At any one time only one USB storage device can be in use. Before inserting a USB storage device, check that no other USB storage device is inserted.
- Only remove USB storage devices after choosing **USB** (global button).
- Use only USB storage devices that are tested and installed by your local Roche service representative.

Computer viruses

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

- Before using a removable storage medium, it should be scanned by an antivirus program.
- 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 disinfect your PC and will check the restoration.

Data backup

Data may get lost due to aging of the hard disk or due to a hard disk failure because of electric power failure.

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