



Ettan™ IPGphor™ 3

Privacy and Security Manual



CONFIDENTIAL - DRAFT - 2022-11-17

Table of Contents

- 1 Introduction 3**
- 2 Privacy and security environment 5**
- 3 Authentication, authorization and audit logging 6**
 - 3.1 Access controls 7
 - 3.2 Audit logging and accountability controls 8
- 4 Patient privacy consent management 9**
- 5 Information protection 10**
- 6 System protection 12**
- 7 Remote access 13**
- 8 Personal information collected by the product 14**
- 9 Additional privacy and security considerations 15**

1 Introduction

About this manual

This manual describes the privacy and security considerations of the use of Ettan IPGphor 3 (IPGphor 3).

Purpose of this manual

This manual describes the expected intended use of IPGphor 3, the privacy and security capabilities included, and how these capabilities are configured.

Scope of this manual

This manual describes the expected intended use of IPGphor 3, the privacy and security capabilities included, and how the product is configured and used appropriately.

Ettan IPGphor 3 is a dedicated system optimized to perform isoelectric focusing using Immobiline™ DryStrip. An integrated high voltage power supply and cooling system minimize focusing time and accurately controlled voltage and temperature give high reproducibility between runs. The Ettan IPGphor 3 control software is used to control the Ettan IPGphor 3 IEF (Isoelectric focusing) unit from a PC.

Introduction to privacy and security

This manual assumes that the reader understands the concepts of privacy and security. Security protects both system and information from risks to confidentiality, integrity, and availability. Security and privacy work together to help reduce risk to an acceptable level. In healthcare, the privacy, security, and safety must be balanced, relating to the intended use of the product.

The customer is encouraged to use risk management procedures to assess and prioritize privacy, security, and safety risks. Using the risk management, the customer can determine how to best leverage the capabilities provided within the product.

Product description

IPGphor 3 Control Software is used to control the IPGphor 3. The software provides data presentation, data storage, and protocol handling. The PC is connected to IPGphor 3 by a USB Type-C cable. IPGphor 3 Control Software controls up to four IPGphor 3 systems at one time, each running a different set of run parameters. The software allows programming and recommended protocols are generated by providing instrument configuration, IPG strip length and pH gradient. The software records the run parameters over time and presents data as graphs and log files. Data is saved or can be exported to Microsoft Excel.

IPGphor 3 is not a medical device and shall not be used in any clinical procedures or for diagnostic purposes.

Safety notices

This user documentation contains safety notices concerning the safe use of the product. See the definition below.



NOTICE

NOTICE indicates instructions that must be followed to avoid damage to the product or other equipment.



IMPORTANT

IMPORTANT indicates instructions that are essential for the software or application to function.

Contact information

For specific privacy and security inquiries, use the contact form found at cytiva.com/contact.

Abbreviations

The following terms and abbreviations are used in this manual:

Term/Abbreviation	Definition
USB	Universal Serial Bus
GxP	Good practice ("x" stands for the various fields)
CFR	Council on Foreign Relations

2 Privacy and security environment

Privacy and security in the environment

IPGphor 3 has been designed for an intended use with the following expectations of privacy and security protection, that should be included in the environment where IPGphor 3 will be used:

- IPGphor 3 instrument is designed for any user to use it in standalone mode of operation, hence user access control is not a primary user requirement for IPGphor 3.
- Results are not classified as sensitive data for this instrument.
- Customers are responsible for security/integrity of data saved on the USB drives.
- This product is not intended for use in any setting that requires compliance with GxP and 21 CFR Part 11 rules.

3 Authentication, authorization and audit logging

About this chapter

IPGphor 3 includes a broad assortment of capabilities to enable privacy and security. This chapter describes the ability and use of these privacy and security capabilities.

3.1 Access controls

Introduction

The access control on IPGphor 3 is used to help control access to customer information on the system. Access control includes user account creation, assigning the privileges, and other features.

Passwords

IPGphor 3 does not support any password policy therefore this section is not applicable.

Identity provisioning

The provisioning of user accounts requires the steps of account creation, maintenance, and removal of the account when it is no longer needed. A user account is created to be used by a specific individual. This user account is associated with access rights, and is recorded in system security log files.

IPGphor 3 does not support user management therefore this section is not applicable.

User authentication

The user authentication step verifies that the user attempting to access the system is indeed the user associated with the specific account. This section describes the administration of the authentication system. IPGphor 3 is deliberately designed with no authentication and data protection. It completely relies on customer security measures. The user must protect data, if considered sensitive with a password protected USB flash drive.

Assigning access rights

Assigning access rights is the administrative process for connecting permissions with user accounts.

IPGphor 3 does not support access control therefore this section is not applicable.

3.2 Audit logging and accountability controls

Introduction

Privacy and security information logging and control provide accountability through security surveillance, auditable records, and reporting.

IPGphor 3 does not support access control therefore this section is not applicable.

4 Patient privacy consent management

Patient privacy

IPGphor 3 does not handle (create, transfer, or store) patient data, therefore the patient privacy consent is not applicable to IPGphor 3.

5 Information protection

About this chapter

This chapter describes privacy and security operations, and contains guidelines for the preparation of a secure environment for IPGphor 3.

Defense in depth

Security operations are best implemented as part of an overall "defense in depth" information assurance strategy. This strategy is used throughout an information technology system that addresses personnel, physical security, and technology. The layered approach of defense in depth limits the risk that the failure of a single security safeguard allows the system to be compromised.

System interconnections

IPGphor 3 does not support for system interconnections therefore this section is not applicable.

Wired network security

Cytiva strongly recommends that IPGphor 3 is operated in a network environment that is separated from the general purpose computing network of the owner's organization. There are many effective techniques for isolating IPGphor 3 on a secure sub-network, including implementing firewall protection, demilitarized zones (DMZs), virtual local area networks (VLANs), and network enclaves.

This section is not applicable for IPGphor 3. IPGphor 3 is a standalone instrument and does not support network connectivity.

Wireless network security

Radio signals are used in a wireless network communication, therefore wireless devices require special security consideration. Effective techniques and tools exist for improving the security of wireless communication. This section describes the characteristics for wireless connections for IPGphor 3.

IPGphor3 does not have wireless connection and therefore it is not a privacy and security concern. IPGphor 3 standalone instrument does not support network connectivity.

Removable media security

IPGphor 3 provides the possibility to use removable media, for example USB storage media. The data generated by IPGphor 3 is unencrypted & data can be saved and stored on the removable media. These storage media and the content on the storage media must be handled according to applicable customer site requirements. Removable media can store of the following data:

- Audit logs
- Saved run data

Data encryption

The instrument does not have any in-built data storage capability. The external storage option (USB) has been provided to store the results. Results are not classified as sensitive data for this instrument, hence there are no additional Privacy & Security Considerations for IPGphor 3 instrument. Users are responsible to use a password protected USB flash drive when saving the data externally.

Backup consideration

IPGphor 3 is not a medical device and does not handle (create, transfer, or store) patient data. Therefore, IPGphor 3 does not contain de-identification (anonymization and pseudonymization) capabilities.

Data integrity

Results are not classified as sensitive data for this instrument.

External connections – Security controls provided by the cloud provider

IPGphor 3 is not hosted on a third party cloud environment. Cloud security controls are not applicable.

6 System protection

Introduction

This chapter describes the guidelines for how to configure and maintain the product in a way that continuously protects privacy and security.

Protection from malicious attacks

The computing environment is increasingly hostile, and threats continue to grow from denial of service attacks and malicious software, including computer viruses, worms, Trojan horses, and other malware. Vigilant defense on many levels is required to keep the systems free from intrusion by malicious software. In most cases, effective protection requires cooperation between Cytiva and our customers.

IPGphor 3 has been designed to work with predefined command response model from display to start software, hence unknown application/malware will not be executed by design. For more information on malicious software protection, refer to the following two white papers by the Joint NEMA/COCIR/JIRA Security and Privacy Committee:

- Defending medical information systems against malicious software, December 2003.
 - Patching off-the-shelf software used in medical information systems, October 2004
- Both documents are available on the following website: <http://www.medicalimaging.org/policy-and-positions/joint-security-and-privacycommittee-2/>.

Whitelisting capabilities

IPGphor 3 is a standalone instrument therefore this section is not applicable. It is the customer's responsibility to use proper anti-virus to protect software from malicious attacks.

Server and workstation security

IPGphor 3 is a standalone instrument therefore this section is not applicable. It is the customer's responsibility to protect the Instrument, USB storage media from being stolen or lost.

Patch management practices

Cytiva will release Patches as timely basis if needed. IPGphor 3 software will be available to download on the Cytiva webpage.

7 Remote access

Introduction

IPGphor 3 does not have any remote access capabilities therefore this section is not applicable.

8 Personal information collected by the product

Personal information

IPGphor 3 is not a medical device and does not handle (create, transfer, or store) patient data. IPGphor 3 does not collect personal information.

9 Additional privacy and security considerations

Additional risks

IPGphor 3 has been designed with privacy and security functionality integrated into the core design. However, there exist privacy and security residual risks that must be mitigated when IPGphor 3 is integrated into the work environment. This section describes some risks that should be imported into the risk assessment of the deployment of IPGphor 3 for proper mitigation.

The instrument is designed for any user to use it in standalone mode of operation, hence user access control is not a primary user requirement for IPGphor 3. IPGphor 3 instrument does not have any in-built data storage capability. The external storage option (USB) has been provided to store the results. Results are not classified as sensitive data for this instrument, hence there are no additional Privacy & Security Considerations for the instrument. Customers are responsible for security of data saved on the external storage device (USB drive).

**Give feedback on this document**

Visit cytiva.com/techdocfeedback or scan the QR code.



cytiva.com

Cytiva and the Drop logo are trademarks of Life Sciences IP Holdings Corp. or an affiliate doing business as Cytiva.

Ettan, Immobililine and IPGphor are trademarks of Global Life Sciences Solutions USA LLC or an affiliate doing business as Cytiva.

Excel and Microsoft are trademarks of Microsoft group of companies.

Any other third-party trademarks are the property of their respective owners.

© 2022 Cytiva

Any use of software may be subject to one or more end user license agreements, a copy of, or notice of which, are available on request.

For local office contact information, visit cytiva.com/contact

29727466 AA V:1 11/2022