cytiva

PrimeView 5.31

Privacy and Security Manual

cytiva.com

Table of Contents

1 Introduction

About this manual

This manual describes the privacy and security considerations for PrimeView™ 5.31.

Purpose of this manual

The purpose of this manual is to describe the expected intended use of PrimeView 5.31, the available privacy and security capabilities of this product, and how these capabilities are configured and used.

Prerequisites

It is assumed that the reader understands the concepts of privacy and security. Privacy is the property of protecting the personal private interests of users. Security protects both system and information from risks to confidentiality, integrity, and availability. Security protects Privacy but also protects widely against these risks. Privacy requires security. One must balance privacy, security, and safety. Most of the time there is no conflict between these three domains of risk. The organization is encouraged to use risk management procedures to assess and prioritize privacy, security, and safety risks. Using risk management, one can determine how to best leverage the capabilities provided in PrimeView 5.31.

Important user information

The PrimeView 5.31 is not a medical device and shall not be used in any clinical procedures or for diagnostic purposes.

2 Privacy and security environment

The Cytiva PrimeView 5.31 has been designed for an intended use with the following expectations of privacy and security protections included in the environment where this product can be used:

The assumption for PrimeView 5.31 related to Privacy and Security elements is as follows:

- It is recommended that the computer hosting PrimeView 5.31 resides in a controlled environment.
- It is recommended to protect mobile devices, that can be moved from a secured environment, following the customer cyber security policies.

3 Privacy and security capabilities

The Cytiva PrimeView 5.31 includes a broad range of capabilities to enable privacy and security. This section describes the capability and the use of these privacy and security capabilities.

Access controls

PrimeView 5.31does not provide any user access control.

Privacy & security audit logging and accountability controls

Privacy and security audit logging and accountability controls supports security surveillance and privacy investigations and reporting.

The audit log resides in the log files under PrimeView 5.31 installation folder. It contains information about usage of the system but not contain any user information as there is no user management.

4 Information protection

This section focuses on privacy and security operations and contains information to guide in the preparation of a secure environment for PrimeView 5.31.

Security operations are best implemented as part of an overall *defense in depth* information assurance strategy that 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 will allow compromise of the system.

Network security

Cytiva strongly recommends that PrimeView 5.31 and ÄKTAprime plus instrument are operated in a secure network environment that is protected from unauthorized intrusion. Implementing firewall protection can be one of several effective techniques to isolate and protect PrimeView 5.31 installation and operations. PrimeView 5.31 is a standalone installation and can be connected to ÄKTAprime plus instrument directly.

Removable media security

PrimeView 5.31does not require any removable media to operate. However, it is strongly recommended that the company policies related to removable media shall be applied to the computer hosting PrimeView 5.31.

Data at rest security

PrimeView 5.31 stores data in a persistent storage, this includes methods, results, log files, and system data. The access to the storage is protected by encryption implemented on files.

De-identification capabilities

PrimeView 5.31 contains no de-identification (anonymization and pseudonymization) capabilities to limit privacy and security risks to sensitive information.

No Privacy Information (PI) is collected by PrimeView 5.31.

Business continuity

A disaster recovery of PrimeView 5.31 database is done by regular restore of database backup. It is recommended that the database backups are stored on a secured media and are made available whenever a restore of the database is required.

Security controls provided by the cloud provider

PrimeView 5.31 is not deployed on cloud.

5 System protection

The System is configured and maintained in a way that protects privacy and security.

5.1 Malicious software protection

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

This product is designed to be used in an environment where commercial Anti-virus software is used to detect the presence of malicious software (virus, Trojan horse, worm, etc.). The use and configuration of the specific AntiVirus software is encouraged.

Note: *During virus scans, the performance of PrimeView 5.31 can be affected and therefore it is recommended to perform scans when the ÄKTAprime plus instrument, which PrimeView 5.31 controls, is not in use. It is recommended to apply the current organizational policies and procedures regarding AntiVirus software.*

For more information on Malicious Software Protection, refer to the following two whitepapers by the Joint NEMA/COCIR/JIRA Security and Privacy Committee:

- Defending Medical Information Systems Against Malicious Software, December 2003, http://www.medicalimaging.org/policy-and-positions/joint-security-and-privacycommittee- 2/
- Patching Off-the-Shelf Software Used in Medical Information Systems, October 2004, http://www.medicalimaging.org/policy-and-positions/joint-security-and-privacycommittee- 2/

5.2 Server and workstation security

PrimeView 5.31 is deployed in a customer controlled environment; hence the customer is responsible for local operational security.

5.3 System (product) change management

The customer is responsible for maintaining the computer hosting PrimeView 5.31. This maintenance includes the following:

- Applying operating system patches
- Applying operating system upgrades
- Applying operating system configuration changes
- Applying operating system routine maintenance
- Applying PrimeView 5.31 patches
- Applying PrimeView 5.31 upgrades
- Applying PrimeView 5.31 configuration changes
- Applying PrimeView 5.31 routine maintenance

Furthermore, any malware protection software installed must also be maintained by the customer. This maintenance includes management of patches, upgrades, configuration change, and routine maintenance. For more information about how to apply malicious software protection, see *Section 5.1 Malicious software protection, on page 8*.

Questions or incident reports regarding cyber security related to PrimeView 5.31 can be done via the appointed Cytiva Key Account Manager or the Cytiva Service Personnel. The appointed Cytiva personnel will take care of the customer case and forward it to the organization within Cytiva responsible for PrimeView 5.31. The case can be of one or more of the following categories:

- A security enhancement is requested in PrimeView 5.31.
- A security incident has occurred related to the usage of PrimeView 5.31.
- A general question about the existence of security related patches for PrimeView 5.31.
- A general question about the availability of online material such as documentation and similar.

6 Remote service

PrimeView 5.31 does not provide support for remote service.

7 Personal information collected by the product

No PI is collected by PrimeView 5.31.

8 Cytiva commitment to data privacy and security

The Cytiva commitment to data privacy and security document can be found in DOC1668119.

cytiva

cytiva.com

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

29328253 AB V:4 04/2021