Ultrasound Workspace 6.0

PHILIPS

Contents

Philips

Contents

1 Introduction

This document describes the supported data formats and the standard hardware and software requirements for Ultrasound Workspace (UWS).

2 Data Compatibility

The following symbols are used in the tables to indicate support or compatibility.

Symbol	Meaning
✔	Supported or compatible
–	Not supported or compatible

Cardiac Imaging

Constraints

	4D LV–ANALYSIS 3D Auto RV 3D Auto CFQ 3D Auto TV	3D Auto MV	4D CARDIO–VIEW	AutoStrain LV/ SAX/RV/LA 2D Auto LV	IMAGE–COM
Minimal frame rate (fps)	10	–	–	–	–
Minimal number of frames per cardiac cycle (frames/cycle)	10	–	–	–	–
Minimal number of frames per clip (frames/clip)	–	3	–	2	–
Minimal number of Stages for stress studies (different values in StageNumber tag)	–	–	–	–	2
Modality for detection of stress echo studies	–	–	–	–	US

2D Data

Modality [2]	Acquisition Protocol	AutoStrain LV/ SAX/RV/LA	2D Auto LV	IMAGE–COM
DICOM 2D US	B–Mode	✔ [6]	✔ [6, 7]	✔
DICOM 2D US	M–Mode, Doppler	–	–	✔
DICOM 2D US	Stress Echo	✔ [6]	✔ [6, 7]	✔
DICOM 2D XA, NM		–	–	✔

3D Data

Modality [2]	Format and Transducers	4D LV– ANALYSIS 3D Auto RV 3D Auto TV	3D Auto MV	4D CARDIO– VIEW	3D Auto CFQ	IMAGE– COM
GE Vivid7 3D, GE E9 3D and GE E95 3D	Supported probes 3V-D, 4V-D, 4Vc-D, 6VT-D, 6Vc-D using raw un-compressed tissue Tissue only (no color Doppler) SW Version (v110-v113) (v201-v204) (v206)	✔	✔	✔	–	✔ [1]
Philips 3D	X8-2t	✔ [3]	✔ [4]	✔ [4]	✔ [8]	✔ [1, 4]
	X7-2t X3-1 X5-1 X7-2 X5-1c X11-4t	✔ [3]	✔ [4]	✔ [4]	–	✔ [1, 4]
	VeriSight Pro ICE	–	–	✔ [4]	–	✔ [1, 4]

Ultrasound Workspace 6.0

Philips

Modality [2]	Acquisition Protocol	Format	4D LV–ANALYSIS 3D Auto RV 3D Auto TV	3D Auto MV 4D CARDIO-VIEW	3D Auto CFQ	IMAGE–COM
Toshiba ARTIDA 3D	Full Volume	Rev 2 and 3	✔ (3, 5)	✔ (3, 5)	–	✔ (1)
Toshiba ARTIDA 3D	Single Volume	Rev 2 and 3	–	–	–	–
CANON 3D		Tissue only (no color Doppler)	✔	✔	–	✔ (1)
HAM Cardiac F75 3D	Normal and Cycle Scan	Tissue only (no color Doppler)	✔	✔	–	✔ (1)
Siemens SC2000 TTE / TEE 3D	4D real time	Tissue only (no color Doppler)	✔	✔	–	✔ (1)

Footnotes for Cardiac Imaging:

1. Requires a separate 3D license.

2. Contact your modality provider regarding special configurations of your ultrasound machine.

3. Supports tissue data only.

4. Supports tissue and color (Doppler, power etc.) data.

5. Datasets containing multiple cardiac cycle data are automatically cropped to one cardiac cycle. For the analysis of Toshiba ARTIDA 3D datasets, only the last cardiac cycle of a multiple cardiac cycle dataset is used. For all other datasets, the first cardiac cycle is used.

6. Support for Philips native single plane 2D data.

7. Segmental Wall Motion requires that the images were taken with supported transducers (X5-1, X5-1c, S5-1), have standard orientations, are not pediatric, and that all three apical views are available. If any of these conditions are not met for images, the corresponding workflow step is grayed out.

8. Supports color data only.

Radiology Imaging

Modality	Acquisition Protocol	Format	4D SONO-SCAN	IMAGE-COM
DICOM multi-frame (handheld)	Manually acquired 2D multi-frame clips	2D multi-frame DICOM (*.dcm or without extension). Specific Format[2]: DicomUS	✓ [3]	✓ [1]
Zonare (Z.ONE)	Wobbler probe acquisition Acquisition modes: 3D/4D static & real-time	DICOM encapsulated Zonare's proprietary 3D/4D volume data. Specific Format[2]: ZONARE_DATA	✓ [3]	✓ [1]
General Electric (Voluson, Logiq)	Wobbler or Matrix probe acquisition Acquisition modes: 4D, Tru3D, Advanced 3D and Easy 3D mode	DICOM encapsulated GE's proprietary (.V00 or .vol) 3D/4D volume data Specific Format[2]: GE_Kretzfile_Wobbler	✓ [4]	✓ [1]
Philips	Matrix probe acquisition Acquisition modes: 3D, 4D	Philips 3D	✓ [3]	✓ [1]
Alpinion (E-Cube)	Acquisition mode: 4D	DICOM encapsulated Philips' proprietary 3D/4D volume data. Specific Format[2]: ALPINION_VOLUME	✓ [3]	✓ [1]
Siemens ABVS	Mechanically acquired 3D data (it is actually spatially calibrated 2D multi-frame data) with a Siemens ABVS device.	2D multi-frame DICOM data (*.dcm or without extension) that includes the frame distance. Specific Format[2]: DicomUS	✓ [3]	✓ [1]

Footnotes for Ultrasound in Radiology:

1. Requires a separate 3D license.
2. As displayed in the DICOM properties dialog of IMAGE-COM.
3. Supports tissue data only.
4. Supports tissue and color (Doppler, power etc.) data.

Image Visualization

Image Visualization on Client Workstations and Standalone Workstations

- No image compression algorithms are used for image visualization.

3 Single Seat Installation

Single Seat Workstation Requirements

This specification is intended to describe the standard hardware and software requirements for application installed and used on a singular workstation.

Operating System

Name	Architecture
Windows 10	x64
Windows 11	x64

For more information, see: https://support.microsoft.com/en-us/lifecycle/search

Hardware

Hardware	Minimum	Recommended
CPU	Intel Core i-Series 6th generation or higher min. 2.2 GHz Base Clock, Dual Core	Intel Core i-Series 10th generation or higher
Memory	16 GB or higher	16 GB or higher
Graphics Card	DirectX 9.0c compatible [1]	DirectX 9.0c compatible [1] Dedicated graphics card recommended
Screen Resolution	1280x1024 or higher	1920x1080
Pointing Device	Mouse with wheel or equivalent input device	
Network	100 Mbit/s or higher	1 Gbit/s or higher

1. DirectX 9.0c feature set is included in higher versions, like DirectX 10, 11, and 12. Intel i-Series CPUs with integrated GPUs are compatible.

Disk Space

The following table is an example of disk space partitioning based on standard values and use cases. This recommendation may vary depending on the infrastructure used and the setup scenario.

Partition		Size
1	Operating System	100 GB (SSD recommended)
2	UWS-Application	100 GB (SSD recommended)
3	UWS-Database + UWS-Archive	minimum 500 GB[1] (SSD recommended)

1. Depending on study throughput

NOTE

In case of PACS Archiving, the size of the file archive should be configured depending on the required time spread, where the data shall be accessible from the Online Cache. Older data will be retrieved from the PACS.

In case of Mass Storage Archiving, the size of the archive depends on the required online availability of the data.

A rough guideline for the size of the UWS-Archive can be estimated in both cases by the following formula:

Minimum size of UWS-Archive [GB] (assumed 25 days of acquiring data/month) = A * T * 25

A = Average Amount of data per day [GB], Input

T = Time spread of availability in Online Cache/Mass Storage Archive [Month]

MSSQL Database

Ultrasound Workspace (6.0 or higher) is delivered with the PostgreSQL database. Existing installations can continue to use MSSQL as a database. The following SQL Server versions are compatible with Ultrasound Workspace and can be used as an alternative to the delivered PostgreSQL database.

Name	Release	End of Support Mainstream [1]	End of Support Extended [1]
SQL Server 2016	2016-01	2021-07	2026-07
SQL Server 2019	2019-11	2025-01	2030-01

1. For more information, see: https://support.microsoft.com/en-us/lifecycle/search

NOTE

- The MSSQL database is not part of the product and must be provided and maintained by the customer.

- Only case insensitive collations are allowed (preferably Latin1_General_CI_AS).

- Ultrasound Workspace uses the TCP/IP protocol to connect to the SQL Server on the default port 1433.

More information can be found in the official documentation:

https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-ver15?view=sql-server-ver15

CAUTION

We urge you to keep your Microsoft SQL version up to date by installing the latest patches after the setup on a regular level, to receive the latest fixes for known vulnerabilities. Retaining an outdated version with known vulnerabilities puts your system at risk of an attack.

CAUTION

We recommend configuring TLS encryption for your SQL server and adjusting the JDBC URL in tomtec.properties accordingly to secure the communication with the database and to prevent the disclosure of private data. For examples and more information on how to setup TLS encryption, see:

- **https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15 for configuring your SQL server, and**

- **https://docs.microsoft.com/en-us/sql/connect/jdbc/connecting-with-ssl-encryption?view=sql-server-ver15 for configuring the JDBC URL**

TLS versions 1.0 and 1.1 are outdated and do not comply with current cybersecurity standards. Therefore, TLS versions 1.0 and 1.1 must not be used for Ultrasound Workspace.

Configuration

Server	
Virus Scanner	The virus scanner has to be disabled for all directories used by Ultrasound Workspace server for the exchange of DICOM data files (e.g. temporary folder of DICOM service and folder of working archive, etc.). For more information, see chapter "File Access and Virus Scanner" on page 21.
Ultrasound Workspace service	Ultrasound Workspace must have sufficient NTFS permissions for the folder that will contain the UWS-Archives: • List folder / read data • Read attributes • Read extended attributes • Create files / write data • Create folders / append data • Write attributes • Write extended attributes • Delete subfolders and files • Delete For a local based file archive the easiest way to grant these permissions is to set the user which is used to run the Ultrasound Workspace … (UWS) service to have "Full access" to the archives folder. This can be done via the "Security" tab of the folder properties. For remote drives, contact the administrator of the remote server to configure the required permissions.
_JAVA_OPTIONS	The environment variable _JAVA_OPTIONS shall not be set as it will influence the JVM used by Ultrasound Workspace. Especially setting maximum heap size below –Xmx4g will lead to startup failure of the Ultrasound Workspace.
PostgreSQL Database	For cyber security reasons, we strongly advise against letting the PostgreSQL database listen on an adapter other than the loopback.

Server	
Minimum Security Requirements	For minimum security requirements you must use a firewall appliance to limit, control or eliminate unwanted access to your local network.
	Furthermore, security safeguards to protect the system against the intrusion of malware (viruses, Trojans, worms) must be in place and must be updated on a regular level.
	In general, access to the software client(s) must be restricted to authorized users only.
	For further security recommendations and more details refer to chapter "Security Considerations" on page 21.

Client	
Page File	The page file of the operating system must remain enabled.
	It is recommended to keep the default settings in the system properties.
	/ Performance options / Virtual memory / : "Automatically manage paging file size for all drives"
Computer Name	The name of the computer shall not exceed 15 characters.
	For more information, see: https://technet.microsoft.com/en-us/library/cc731383.aspx https://technet.microsoft.com/en-us/library/cc726016(v=ws.10).aspx
PDF Viewer	Adobe Acrobat Reader compatible with the installed operating system must be used.
Media Feature Pack	For Windows 10 N versions a separate installation of the Media Feature Pack is required.
WebView2	Microsoft Edge WebView2 Runtime version 119 or higher is required.
Screen Scaling	Recommended system scaling factor should be configured.
Monitor	We strongly recommend an aspect ratio of 4:3 or 16:9. The application runs in full screen mode. It is not possible to change the size of the window. Therefore, two monitors are required to display the image review and reporting side by side. Tools that allow the virtual desktop to be split are not supported.
Energy Settings	The energy saving mode must be set to "Balanced". The device must always be connected to a power source and have the highest power settings.

Backup Strategy

A backup strategy needs to be set up for every installation individually. To restore the system completely it is recommended to back up the database, the complete file archive and all configuration files.

4 Server Client Installation

Server client installations are for multi-seat configurations which supports multiple clients at the same time.

Philips

Client Workstation Requirements

This chapter describes the standard hardware and software requirements for all scenarios where the client application is installed on a workstation system with an external database such as an Ultrasound Workspace server or third-party integrations.

Operating System

Name	Architecture
Windows 10	x64
Windows 11	x64

For more information, see: https://support.microsoft.com/en-us/lifecycle/search

Hardware

Hardware	Minimum	Recommended
CPU	Intel Core i-Series 6th generation or higher min. 2.3 GHz Base Clock, Dual Core	Intel Core i-Series 10th generation or higher
Memory	8 GB or higher[1]	16 GB or higher
Graphics Card	DirectX 9.0c compatible [2]	DirectX 9.0c compatible [2] Dedicated graphics card recommended
Screen Resolution	1280x1024 or higher	1920x1080
Pointing Device	Mouse with wheel or equivalent input device	
Network	100 Mbit/s or higher[1]	1 Gbit/s or higher

1. For large image volumes, high frame rate studies, or uncompressed data, we recommend using the recommended setting for optimal system performance.

2. DirectX 9.0c feature set is included in higher versions, like DirectX 10, 11, and 12. Intel i-Series CPUs with integrated GPUs are compatible.

Disk Space

Software	Size
Client Software	4 GB (SSD recommended)

Configuration

Client	
Page File	The page file of the operating system must remain enabled.
	It is recommended to keep the default settings in the system properties.
	/ Performance options / Virtual memory / : "Automatically manage paging file size for all drives"
Computer Name	The name of the computer shall not exceed 15 characters.
	For more information, see: https://technet.microsoft.com/en-us/library/cc731383.aspx https://technet.microsoft.com/en-us/library/cc726016(v=ws.10).aspx
PDF Viewer	Adobe Acrobat Reader compatible with the installed operating system must be used.
Media Feature Pack	For Windows 10 N versions a separate installation of the Media Feature Pack is required.
WebView2	Microsoft Edge WebView2 Runtime version 119 or higher is required.
Screen Scaling	Recommended system scaling factor should be configured.
_JAVA_OPTIONS	The environment variable _JAVA_OPTIONS shall not be set as it will influence the JVM used by Ultrasound Workspace.
	Especially setting maximum heap size below –Xmx4g will lead to startup failure of the Ultrasound Workspace.
Minimum Security Requirements	For minimum security requirements you must use a firewall appliance to limit, control or eliminate unwanted access to your local network.
	Furthermore, security safeguards to protect the system against the intrusion of malware (viruses, Trojans, worms) must be in place and must be updated on a regular level.
	In general, access to the software client(s) must be restricted to authorized users only.
	For further security recommendations and more details refer to chapter "Security Considerations" on page 21.

NOTE

The user manuals are provided as PDF files. If you do not have a PDF reader application installed, you can download Adobe Reader from the following website: www.adobe.com

Web Client Requirements

Officially Supported Browser

Windows Based Browser	Architecture	Supported Build
Google Chrome / Edge Chromium	x86, x64	>=104

NOTE

For security reasons we recommend that you always use the latest version of the browser.

Server Requirements

This chapter describes the standard physical and virtual hardware and software requirements for server applications installed in a network server and client infrastructure based on a standard clinical use case. For further scaling considerations, refer to chapter "System Scaling" on page 20.

Operating System

Name	Architecture	Release	End of Support Mainstream [1]	End of Support Extended [1]
Windows Server 2016	x64	2016-09	2022-01	2027-01
Windows Server 2019	x64	2018-11	2024-01	2029-01

1. For more information, see: https://support.microsoft.com/en-us/lifecycle/search

NOTE

The language of the operating system installed on the server must be English.

MSSQL Database

Ultrasound Workspace (6.0 or higher) is delivered with the PostgreSQL database. Existing installations can continue to use MSSQL as a database. The following SQL Server versions are compatible with Ultrasound Workspace and can be used as an alternative to the delivered PostgreSQL database.

Name	Release	End of Support Mainstream [1]	End of Support Extended [1]
SQL Server 2016	2016-01	2021-07	2026-07
SQL Server 2019	2019-11	2025-01	2030-01

1. For more information, see: https://support.microsoft.com/en-us/lifecycle/search

Philips

NOTE

- The MSSQL database is not part of the product and must be provided and maintained by the customer.
- Due to limitations the Express Edition of the MS SQL Server cannot be used for Client Server Installations.
- Only case insensitive collations are allowed (preferably Latin1_General_CI_AS).
- Ultrasound Workspace uses the TCP/IP protocol to connect to the SQL Server on the default port 1433.

More information can be found in the official documentation:

https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-ver15?view=sql-server-ver15

CAUTION

We recommend configuring TLS encryption for your SQL server and adjusting the JDBC URL in tomtec.properties accordingly to secure the communication with the database and to prevent the disclosure of private data. For examples and more information on how to setup TLS encryption, see:

- **https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15 for configuring your SQL server, and**
- **https://docs.microsoft.com/en-us/sql/connect/jdbc/connecting-with-ssl-encryption?view=sql-server-ver15 for configuring the JDBC URL**

TLS versions 1.0 and 1.1 are outdated and do not comply with current cyber security standards. Therefore, TLS versions 1.0 and 1.1 must not be used for Ultrasound Workspace.

Hardware (physical or virtual)

Hardware	Minimum	Recommended
CPU	Intel Core i-Series 6th generation or Intel Xeon E-series (Skylake) or higher 8 Cores 2.2 GHz clock speed or higher	CPU Intel Xeon E-series or higher
Memory	16 GB or higher	32 GB or higher
Graphics Card	DirectX 9.0c compatible [1, 2]	DirectX 9.0c compatible [1, 2]
Network	100 Mbit/s or higher[3]	1 Gbit/s or higher

1. Only required when client applications are used on the server, otherwise no specific GPU required.

30001400S871_A/ * JUN 2024

Philips

2. DirectX 9.0c feature set is included in higher versions of DirectX like version 10 and above. Intel i-Series CPUs with integrated GPUs are compatible.

3. For large image volumes, high frame rate studies, or uncompressed data, we recommend using the recommended setting for optimal system performance.

Disk Space

The following table is an example of disk space partitioning based on a standard departmental use case where a server is used to store and manage image data. This recommendation may vary depending on the archiving workflow, infrastructure used, and setup scenario such as Measurement Mapping service or license service only. Contact your representative for a recommendation tailored to your needs.

Partition		Size
1	Operating System	100 GB (SSD recommended)
2	UWS-Application	100 GB (SSD recommended)
3	UWS-Database + UWS-Archive	minimum 500 GB[1] (SSD recommended)

1. Depending on study throughput

NOTE

In case of PACS Archiving, the size of the file archive should be configured depending on the required time spread, where the data shall be accessible from the Online Cache. Older data will be retrieved from the PACS.

In case of Mass Storage Archiving, the size of the archive depends on the required online availability of the data.

A rough guideline for the size of the UWS-Archive can be estimated in both cases by the following formula:

Minimum size of UWS-Archive [GB] (assumed 25 days of acquiring data/month) = A * T * 25

A = Average Amount of data per day [GB], Input

T = Time spread of availability in Online Cache/Mass Storage Archive [Month]

Configuration

Server	
TCP/IP Ports	Port 80 and 51080 must be accessible from all client workstations. Ports 2100 and 50145 must be accessible for HL7/DICOM communication. Port 1433 is used to connect to the SQL Server. Port 5432 is used to connect to the PostgreSQL server (localhost only).
Virus Scanner	The virus scanner has to be disabled for all directories used by Ultrasound Workspace server for the exchange of DICOM data files (e.g. temporary folder of DICOM service and folder of working archive, etc.).
	For more information, see chapter "File Access and Virus Scanner" on page 21.

Philips

Server	
Ultrasound Workspace Service	Ultrasound Workspace must have sufficient NTFS permissions for the folder that will contain the UWS-Archives: - List folder / read data - Read attributes - Read extended attributes - Create files / write data - Create folders / append data - Write attributes - Write extended attributes - Delete subfolders and files - Delete For a local based file archive the easiest way to grant these permissions is to set the user which is used to run the Ultrasound Workspace … (UWS) service to have "Full access" to the archives folder. This can be done via the "Security" tab of the folder properties. For remote drives, contact the administrator of the remote server to configure the required permissions.
_JAVA_OPTIONS	The environment variable _JAVA_OPTIONS shall not be set as it will influence the JVM used by Ultrasound Workspace. Especially setting maximum heap size below –Xmx4g will lead to startup failure of the Ultrasound Workspace.
Minimum Security Requirements	For minimum security requirements you must use a firewall appliance to limit, control or eliminate unwanted access to your local network. Furthermore, security safeguards to protect the system against the intrusion of malware (viruses, Trojans, worms) must be in place and must be updated on a regular level. In general, access to the software client(s) must be restricted to authorized users only. For further security recommendations and more details refer to chapter "Security Considerations" on page 21.

CAUTION

The software requires ports 80 and 51080 to be accessible from all client workstations. Ports 2100 and 50145 must be accessible for HL7/DICOM communication. Port 1433 is used to connect to the SQL Server. Port 5432 is used to connect to the PostgreSQL server (localhost only). Otherwise, all idle ports should be closed by your firewall to limit access to your system.

Backup Strategy

A backup strategy needs to be set up for every installation individually. To restore the system completely it is recommended to back up the database, the complete file archive and all configuration files.

5 License Server

This chapter describes the standard software requirements for all scenarios in which the license server is installed as a separate component for third-party integrations.

Operating System

Name	Architecture	Release	End of Support Mainstream [1]	End of Support Extended [1]
Windows Server 2016	x64	2016-09	2022-01	2027-01
Windows Server 2019	X64	2018-11	2024-01	2029-01

1. For more information, see: https://support.microsoft.com/en-us/lifecycle/search

NOTE

The language of the operating system installed on the server must be English.

Configuration

⚠ **CAUTION**

The license server requires port 50002 to be accessible from all client workstations. Otherwise, all idle ports should be closed by your firewall to limit access to your system.

6 System Scaling

The system is designed to support departmental use cases and a workstation and server client based scenario. In case you plan to use the system in a multi-department multi-site scenario, additional system scaling considerations shall be considered which are highly dependent on the user workflow and use case. Contact your service representative for further information.

7 System Virtualization

The product supports server virtualization only. All clinical applications, which display or render data, must run on physical hardware with a rendering engine. In case image display and rendering will be used for maintenance purposes on virtual servers, a 3D acceleration support and WebGL is required.

NOTE

Virtualization of clients, e.g. clinical applications, is not supported.

Philips

8 File Access and Virus Scanner

For performance reasons, the virus scanner shall be deactivated for all directories used by Ultrasound Workspace server. On-access scan exclusions shall be configured for the data archive directories used as well as for log file and temp directories that are created after the installation of Ultrasound Workspace.

Installations that are integrated into third-party systems use additional configurable directories for the exchange of DICOM data. For performance reasons, these directories should also be excluded from the on-access scan of the virus scanner. For information about the on-access scan exclusions, contact your service representative.

9 Security Considerations

⚠ **CAUTION**

The product must only be used within a secured, private network environment (e.g. only accessible from software clients inside of the network) that meets the minimum security requirements as defined for the specific setups within this document (see chapters "Single Seat Installation" on page 9 and "Server Client Installation" on page 13 respectively). Using the product otherwise is not secure and results in severe risk for disclosure of sensitive data or the integrity of the system in general. Philips is not responsible for any security incidents that may result from using the product beyond these restrictions.

Security standards like user identification, password handling or automatic timed session terminations are offered by this product. Further actions to support cybersecurity (e.g. security updates, malware protection or network communication protection) need to be taken by the local IT or Security/Cybersecurity responsible at user site.

Protection can only be realized if you implement a comprehensive, multi-layered strategy (including policies, processes, and technologies) to protect information and systems from external and internal threats. Following industry standard practice, your strategy should address physical security, operational security, procedural security, risk management, security policies, and contingency planning. The practical implementation of technical security elements varies by site and may employ several technologies, including firewalls, virus-scanning software, authentication technologies, etc. As with any computer-based system, protection must be provided such that firewalls and/or other security devices are in place between the medical system and any externally accessible systems.

Following security and industry best practices, security strategies should address:

- Physical security: e.g. locks, cameras, keycards, sensors, and so on, for restricting unauthorized access.

- Operational security: e.g. access/authorization controls, change management, network segmentation based on data classification, password protection of BIOS, disabling booting from external drives like USB, disabling unused ports/services.

- Procedural security: e.g. unattended workstation locking, no sharing of access credentials, termination checklists, risk management (that is, performing risk assessments and mitigating identified risks), and so on.
- Security policies: e.g. ensuring that the system service documentation and media, CDs, and DVDs are securely stored; and that systems are in line with your IT security policies.
- Training and awareness;
- Contingency planning;

When installing a new system or upgrading an existing system, it is important to work with your IT department to ensure that the proper security measures and policies are in place.

User Authentication

Ensure that Ultrasound Workspace host PCs are configured for user authentication and that the individuals using Ultrasound Workspace host PCs have a user name and password. You can use this information to protect the data in the folders and individual files. Use strong passwords for access to Ultrasound Workspace host PCs and data.

Operating System

Ensure that the operating system and applications on Ultrasound Workspace host PCs are kept current with patches, updates, and upgrades.

Network Security

If the Ultrasound Workspace host PC is connected to a local area network, the network should be securely configured, providing protection against computer viruses and other harmful code or traffic. Ensure that the local area network uses appropriate protection, such as using only secure wireless technologies, firewalls, intrusion-detection systems, and virus scanners.

Network Encryption

⚠ **CAUTION**

To improve security the operator can insulate the product by adding a proxy supporting encrypted communication (HTTPS).

NOTE

Contact your service representative for further information.

Firewalls

The use of a firewall appliance as a good security practice is highly recommended. It is advised that the customer takes proper precautions to limit, control or eliminate unwanted access.

You can obtain a list of the ports, services and protocols that must be configured in the firewall from your service representative.

Remote Administration

If remote administration is used on the Ultrasound Workspace host PCs, ensure that they are configured for secure remote administration.

Malware Prevention and Detection

Security safeguards to protect the system against the intrusion of malware (viruses, Trojans, worms,) are recommended. Malware prevention software should be configured to receive automatic updates. Additionally, be sure to adhere to local IT policies and procedures regarding malware infection, which may include disconnecting from the network until the situation is resolved.

Operational Security

CAUTION

To keep the system secure, it is recommended to follow proper operational security measures like:

- **Password-protected BIOS**
- **Disallow booting from external drives in the boot order.**
- **Disable unused I/O device interfaces.**
- **Disable unused services and ports.**
- **Control physical access to the product. Only authorized personnel should have access.**
- **Create and enforce policies that ensure unauthorized users cannot gain access.**

Physical Security and Limited Access to Systems

CAUTION

It is important to consider physical security measures like keeping the system in a secure location, limiting access to only authorized personnel, proper locking measures, card-key or other access limitations, and so on. Access to systems must be limited to authorized users and controls must be implemented to ensure that unauthorized users cannot gain access.

NOTE

Contact your service representative for further information.

Protecting Personal Information

It is essential that policies and procedures for the proper handling of personal or sensitive data are in place. Consider the confidentiality, integrity, and the availability of the types of data. Each organization using this product must provide the protective means necessary to safeguard personal information consistent with each country law, code and regulation, and consistent with the company policies for managing this information.

Although the handling of personal data is outside the scope of this document, in general, each organization is responsible for identifying the following:

- Who has access to personal data and under what conditions an individual has the authorization to use this data?
- How is the data stored, under what conditions and by whom it is stored?
- How is the data transmitted and under what conditions is this data transmitted?

CAUTION

When disposing of the hard drive, first purge all sensitive data using software capable of DoD 5220.22-M standards, or comparable.

Media such as CDs, DVDs, USB drives, and printouts must be disposed of in a secure manner when they are no longer needed, since they might hold sensitive information.

Philips

Protecting Personal Health Information

⚠️ **CAUTION**

Protecting personal health information is a primary part of a security strategy. Considering the nature of the product, the information stored is highly personal and sensitive and should be protected following HIPAA or Council of the European Union security and privacy rules.

The system does not encrypt patient health information when stored. Unencrypted patient health information will be present in the system files, backup files, and files saved to primary, auxiliary, and portable storage devices. Thus, particular care must be taken with this information when designing backup, archiving, and disaster recovery plans to ensure the utmost security and confidentiality.

Additionally, industry standard methods and best practices of applying disk level encryption may be applied to protect data at rest. Philips recommends a careful examination of the encryption method as it may affect the overall performance of the system.

Take measures to compensate for resource drain when encrypting\decrypting files or data. This will need to be identified during the beginning stages of implementation, prior to server build.

⚠️ **CAUTION**

When disposing of the hard drive, first purge all sensitive data using software capable of DoD 5220.22-M standards, or comparable.

Media such as CDs, DVDs, USB drives, and printouts must be disposed of in a secure manner when they are no longer needed, since they might hold sensitive information.

About the EU Directives

If applicable, your facility's security strategy should include the practices set forth in the Directive on Privacy and Electronic Communications (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002) concerning the processing of personal data and the protection of privacy in the electronic communications sector. In addition, your facility should also consider any additional, more stringent standards put forward by any individual EU countries; that is, Germany, France, and so on. For more information, visit http://eur-lex.europa.eu/homepage.html

About Setting up a Testing Environment

Customers are encouraged to put policies in place to maintain proper operating systems, anti-virus, and Microsoft security updates and service packs, driver updates, new hardware and changes to existing hardware, and so on. Ultrasound Workspace is a software-only product. Proceed with caution when you make any changes to any part of the system. Be sure to set up a test environment that mimics the current environment for testing changes to the system before deploying the changes into the live environment. Real patient data should not be used for the test/demo environment. Any such test setup must use de-identified data only.

Philips

About HIPAA Rules

If applicable, your facility's security strategy should include the standards set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), introduced by the United States Department of Health and Human Services. You should consider both the security and the privacy rules and the HITECH Act when designing policies and procedures. For more information, visit https://www.hhs.gov/hipaa/index.html.

Further Security Information

User Accounts

We suggest user accounts (example: for installation, monitoring, troubleshooting, remote access purpose, runtime and emergency account) with proper read/write/execute access levels to shared resources (shared network drives, services, database) be created as per Hospital's IT policy.

Network

⚠ **CAUTION**

The product relies on the existing network infrastructure to provide security. All DICOM interfaces use unencrypted DICOM. All HL7 interfaces use unencrypted HL7.

Disclosure

TeamDev JxBrowser and Microsoft WebView2 are used within the product. JxBrowser and WebView2 may send data back to Google or Microsoft. Thus, you might detect unexpected traffic from the system. This is normal. To our best knowledge, no sensitive data is transferred by JxBrowser. Nevertheless, you can block the traffic with your firewall without any impact on the behavior of the product.

www.philips.com/healthcare

|▲▲|

Philips Ultrasound LLC
22100 Bothell Everett Hwy
Bothell, WA 98021-8431
USA

| EC | REP |

Philips Medical Systems Nederland B.V.
Veenpluis 6
5684 PC Best
The Netherlands

CE 2797