# VOLUSON SECURITY & PRIVACY

## PROTECT YOURSELF AND YOUR PATIENTS

With the advancement of digital capabilities including wireless technology and software in healthcare, the possibility that a practice will face cyber threats and/or data breaches is imminent. Being a computer based system, ultrasound devices can be vulnerable to security threats which could impact safety, effectiveness, and data security of the device.

At GE Healthcare, you and your patients' safety and data privacy are a top priority. We work diligently to ensure Voluson™ ultrasound systems rely on the latest and most advanced security levels with the flexibility needed to efficiently manage your practice.

gehealthcare.com

# CYBERSECURITY IS MORE THAN ANTI-VIRUS PROTECTION

## DESIGNING THE MOST SECURE ULTRASOUND

GE Healthcare has created a strategic framework called Design Engineering for Privacy and Security (DEPS) which is utilized in our product development. It begins by assessing the privacy and security risk and providing guidance to the ultrasound system design team. The Voluson ultrasound systems contain the following design elements to protect you out of the box.

- Windows® 10 operating system and ability to update with the latest security patches when Microsoft makes them available. This update can happen after engineering evaluation and testing for system compatibility
- Access a dedicated portal to download urgent software fixes
- Software services embedded in the operating system which are not required to run on an ultrasound system are removed or disabled
- Network ports not required for data communication are disabled to minimize the risk of threat invasion
- Protection against USB-borne attacks by disabling any auto-run functionality and by scanning the USB stick for security threats immediately when connected
- For means of anti-virus protection, we apply whitelisting – limiting software programs that can run on a system to those identified and approved in advance. Unknown, potentially malicious software will not be executed to protect the ultrasound system
- An advantage of a big company like GE is that it has a strong central security team that constantly monitors for new security threats and communicates with Voluson engineers to design and implement additional security updates as needed

## MAINTAINING PATIENT PRIVACY AND SECURITY

Protecting the systems against malware or other cyber attacks is one aspect of system security, but it is also important to protect locally stored information against theft or corruption. This is where data protection measures come into play.

### Secure sharing

- Locally stored patient information can be protected with Hard Drive (HD) encryption – AES Encryption with 256 bit length
- Voluson ultrasound systems use encrypted DICOM® Communication Capability (TLS) – TLS is an encryption technique to ensure that the data being passed across your networks cannot be intercepted and read during transmission to ViewPoint,™ PACS, HIS, etc.*
- Securely share ultrasound information via the cloud with Tricefy™**

### User management

- Easily manage ultrasound system access for multiple users with individual log on credentials – define adjustable access levels to system functionality based on user need
- User access credentials can be managed remotely by means of a Lightweight Directory Access Protocol (LDAP) interface, particularly targeted towards the use in larger institutions
- Voluson can monitor and record any security-related activities including user logins, data handling and networks connections generating an audit trail and usage log

Available on Voluson Systems BT18 and above.

*Check PACS and HIS system for TLS encryption availability.

**Not available in all countries.