DEL MEDICAL

CyberSecurity

PROTECTION

Helping You Stay Secure

To provide exceptional patient care without interruption, it is critical for health care providers to have a secure environment, protected against cyberthreats such as viruses or ransomware. UMG/DEL MEDICAL takes our partnership in this seriously and is committed to providing safe, reliable, and secure systems. We deliver product security that helps you achieve compliance with Health Insurance Portability and Accountability Act (HIPAA). Together, we can increase security and privacy.

Design and Testing

UMG/DEL MEDICAL designs and tests systems according to internationally accepted standards and procedures. Our design aim is to minimize the attack surface by granting access only to the authorized users and processes needed to perform their necessary tasks or functions. We continually evaluate the vulnerability of our systems and apply the latest software and security updates to prevent and remediate any critical threats.

People

In the challenging cybersecurity environment, having a company culture that values secure operations is important. We provide cybersecurity and HIPAA awareness and role-specific training for all management, R&D, operation, service and support personnel.

Adherence to Standards and Guidance

UMG/DEL MEDICAL adheres to and supports industry standards for cybersecurity including:

- Publication of industry-standard MDS2 (Manufacturers Disclosure Statements for Medical Device Security) disclosure statements for all current systems, available on our web site, at the links below. These statements, as standardized by Healthcare Information and Management Systems Society (HIMSS) and National Electrical Manufacturers Association (NEMA), provide information to assess the security of our systems.
- FDA guidance for Management of Cybersecurity in Medical Devices.
- Encryption of data in motion and at rest.
- Implementation of Operating System policies for updates using Group Policy Objects (GPO) consistent with Department of Defense Information Assurance Security Technical Implementation Guides (STIGS).

Constant Vigilance and Intelligent Threat Response

To protect from new threats that emerge and as operating system updates are issued, UMG/DEL MEDICAL routinely runs vulnerability scans of our systems. The systems receive Operating System and Security updates through the automated Windows Update process to assure they are always patched against new, known vulnerabilities. We evaluate each update to assure security remains intact and functionality unaffected. For critical updates or threat management requiring intervention, a service bulletin is issued to our service providers.

Contact

For the latest information on cybersecurity or to report any vulnerabilities, please contact UMG/DEL MEDICAL's support center at 800-800-6006 or visit our website at www.delmedical.com. The UMG/DEL MEDICAL support team can assist in advising all recommended security measures and configuration items specific to any UMG/DEL MEDICAL hardware or software application.

Specific Workstation and Server Security Methods

Disclosure Statements

We have published industry standard MDS2 forms (Manufacturers Disclosure Statements for Medical Device Security) for all current systems, available on our web site, at the links below. These statements, as standardized by HIMSS and NEMA, provide information to assess the security of our systems.

Please visit delmedical.com/support for current MDS2 forms.

User Login

User-level privileges are locally defined and enforced.

Administrative passwords are not typically provided to untrained service personnel or general users to prevent the ability to access areas of potential vulnerability.

EvoView PACS

User names, passwords, and specific user roles can be created and modified at the customer's request.

DELWORKS EDR Acquisition Software

DELWORKS starts automatically and disables return access to the windows desktop unless the user has an Administrative account privilege.

Session Timeouts

Session Timeouts are employed based on the typical needs of the application.

These defaults are set solely dependent on the type of application and can also be modified at any time per a customer's request.

EvoView PACS

Enables session timeouts which are configurable based on the user, workstation, or user role.

DELWORKS EDR Acquisition Software

Due to the sometimes urgent needs of the acquisition software application, there is currently no session time-out in place by default.

Timeouts may be enabled per user request.

Hard Disk Encryption

EvoView PACS

As a storage system, file encryption of data at rest is enabled via BitLocker full encryption, using method XTS-AES 256-bit. This provides encryption of all content within the disk storage. Additionally, EvoView systems adhere to the Federal Information Processing Standards (FIPS) 140-2 standard to help secure against unwanted tampering.

DELWORKS EDR Acquisition Software

As a storage system, file encryption of data at rest is enabled via BitLocker full encryption, using method XTS-AES 256-bit. This provides encryption of all content within the disk storage.

Physical Lock

Workstation and Server hardware include features such as tamper protection that can be enabled which will keep a log or provide notification if a cover is removed at an unexpected time. The hardware can also be physically locked to prevent opening at the back of the hardware chassis.

Network Security

UMG/DEL MEDICAL Workstation and Server systems utilize Windows Firewall to protect against any potentially malicious inbound (or outbound) traffic. All ports are closed unless critically necessary for the operation of the application. Firewall exceptions can be made and ports can be opened as necessary, provided they do not affect system stability or functionality. Exceptions should only be considered for critical application need.

Common reasons for network security modifications include connectivity with other site locations, applications or devices, and external viewing access for PACS systems. The UMG/DEL MEDICAL support team should be contacted for any such need along with the site's IT and Security team.

Antivirus Software

UMG/DEL MEDICAL Workstation and Server systems use Windows Defender by default for antivirus and anti-malware. Other antivirus/anti-malware applications may be used per customer preference and can be instituted any time with the assistance of the UMG/DEL MEDICAL support team. A list of necessary exclusions can be provided based on the Application type and need.

Windows Security Updates

Windows Security Updates are enabled with a 30-day delay so that DEL MEDICAL may validate that updates do not cause any system failures. Updates are then automatically applied after testing and validation has been completed by the UMG/DEL MEDICAL support team.

New York
28 Calvert Street
Harrison, NY 10528
(Tel) 800.261.9808
(Fax) 914.835.6111

Illinois
241 Covington Drive
Bloomingdale, IL 60108
(Tel) 800.800.6006
(Fax) 847.288.7011

www.delmedical.com