

CYBERSECURITY & DATA PROTECTION

Securing laboratory equipment from cyber attack shouldn't be your concern

Selecting the right partner is critical

GRIFOLS

In today's connected world, everyone—including your healthcare organization—is susceptible to cyber attack

Do your laboratory devices protect your data and day-to-day work?

Medical staff require an easy-to-access, secure network that offers tranquility that patient data is protected. Cybersecurity solutions are complex, and selecting the right partner is crucial.

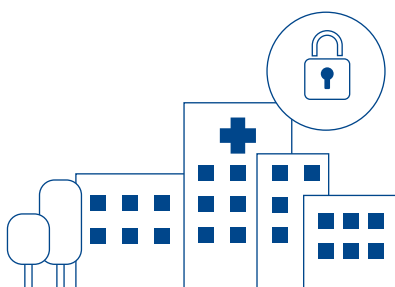
Grifols designs diagnostic systems with cybersecurity in mind—because we are committed to protecting your organization from security breaches.

We put information security procedures in place, and you get peace of mind knowing that the confidentiality, integrity, and availability of your data and systems are in good hands.

We are ISO 27001* certified, which is the highest level of accreditation for data security, in the post-market interventions through our professional team of Commercial Technical Support.

* ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

When we develop solutions for your laboratory, cybersecurity is one of our highest priorities



RESPONSIBLE APPROACH TO SECURITY

Cybercriminals focus on healthcare as a target for cyberattacks. Grifols Information Security Office oversees the organization's cybersecurity policy.

We constantly assess risks and impacts across the entire life-cycle of our products.

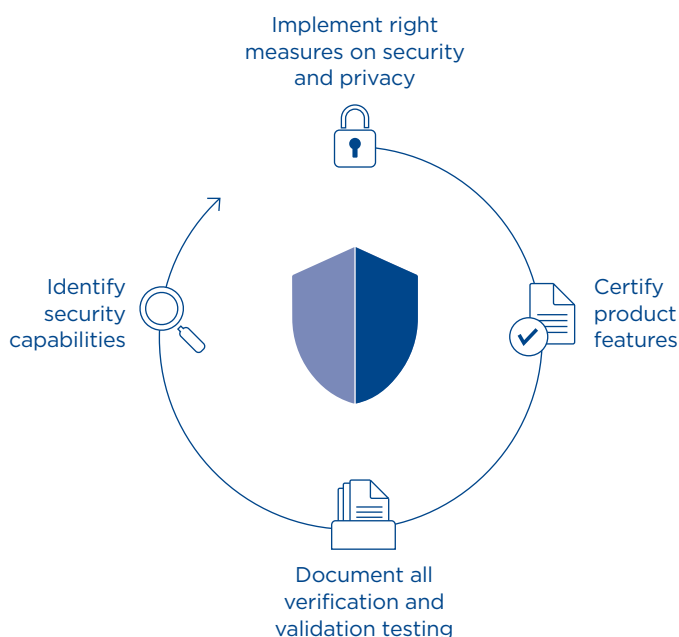
We secure our systems for your tranquility.

Security by Design Privacy by Default

Grifols designs transfusion medicine systems with security in mind to make it harder for attackers to compromise your systems. We use security by design and privacy by default principles throughout the Grifols development process to assure a secure system that prevents unwanted access to your system.

Our focus on the latest cybersecurity principles forms the foundation of security within our systems. Our development life cycle integrates security at every phase of development, from concept to deployment to maintenance and beyond.

Implementing design control systems is the core of secure management:



Network segregation

Your diagnostic system should be under control to ensure it transmits patient data in a safe, secure manner.

An enabled firewall in our systems isolates your instrument from the network, allowing only configured input and output data streams.



Malware detection protection

In our diagnostic systems, whitelisting applications such as Microsoft AppLocker blocks malware attacks and helps assure system integrity.



Confidentiality in transit

Connections and communications across information systems may be encrypted to help ensure that transmitted data remains secure.



User access controls

Through authentication and authorization, access control policies ensure that authorized users have access only to the data they need for their work. You are secure with auto-logout, password protection, and role-based access controls that are all logged for audit when you need to review.

By protecting your data, we protect you



Secure Remote Connectivity

Grifols Secure Remote Connectivity (SRC) is a compliant, secure connectivity tool that allows our Technical Support team to remotely access and troubleshoot instruments. Grifols SRC is a customized version of BeyondTrust Secure Remote Support technology* that is proven to offer very high security. It ensures you remain in control of a confidential peer-to-peer service.

We establish an extra layer of security by avoiding any physical foothold on your network, which is often required by standard VPN support connections.



Security Updates

No one can anticipate every emerging cyber threat. Frequent risk assessment helps laboratories feel safe against the latest threats to data systems. Grifols commits to meticulously assessing security updates before release, aiming at no impact on performance, including those related to off-the-shelf software.



ISAO** Membership

We continuously improve and prepare for your needs. We approach data security seriously, which is why we are an active member of MedISAO, a community of medical device companies that shares information for better tools to offset threats.

* BeyondTrust meets with the data privacy criteria outlined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. It also complies with the major cybersecurity standards, including ISO 27001 certification, SOC 2 Type 1, ISO/IEC 15408, PCI DSS, and FIPS 140-2.

** (Information Sharing Analysis Organization)

MedISAO is an organization composed of members of the medical device community that is dedicated to improving the security of medical devices through education, awareness, and advocacy.



Diagnostic Support & Services provides solutions that allow laboratory professionals to focus on high-quality patient care. Our mission is simple—be there for you so you can deliver reliable results on time and provide peace of mind.

diagnostic.grifols.com

GRIFOLS

Grifols Asia Pacific Pte Ltd
460 Alexandra Road
#09-01 mTower
Singapore 119963
Tel: +65 6708 7166
Fax: +65 6735 2607

Grifols International, S.A.
Parc Empresarial Can Sant Joan
Av. de la Generalitat, 152-158
08174 Sant Cugat del Vallès
Barcelona - España
Tel. +34 935 710 500