
Your eyes only
Cybersecurity and privacy for MAC™ 5
Electrogardiograph System
MAC 5 is built on the most secure resting ECG platform we have ever designed. It is designed to provide patients and providers with the peace of mind that comes from knowing their information is safe and secure.
gehealthcare.com

Medical cybersecurity is more than just anti-virus protection

Protecting our institutions, staff, and patients requires more than anti-virus protection. It takes strategy and collaboration. By working together we can not only protect individual devices, but also enhance overall system security.

The basic framework

In the design of the MAC 5 ECG system, we have developed a comprehensive approach to cybersecurity:

- GE Healthcare's strategic approach, known as DEPS (Design Engineering for Privacy and Security)
- Software development maturity
- Product security posture
- Ongoing security vigilance
- Customer communication

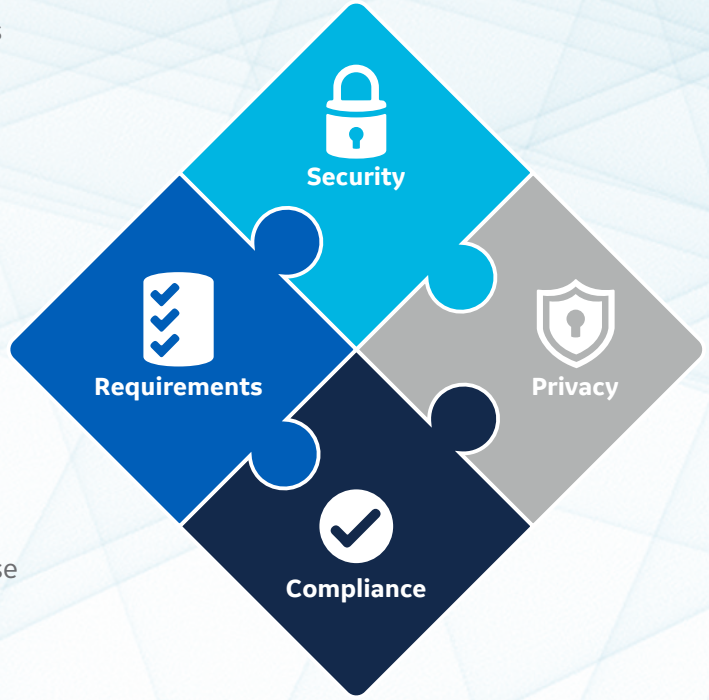
DEPS – A comprehensive approach to security

Design Engineering for Privacy and Security is the strategic framework that GE has adopted for all of its products, including the MAC 5.

DEPS starts with assessing the risk presented in the use of the system and then gives guidance to the design team about how to implement proper security and privacy controls by asking questions such as:

- Is remote access possible?
- Are elements of the design connected to the cloud?
- Is it a mobile device?
- Does it collect, use, or store personal health information?
- Is it being used in medical urgent situations (low barriers to access)?
- Is high availability required?
- Is data integrity critical to patient care?
- Is there wireless connectivity?
- Is it being transported between multiple sites?
- Does it have removable media like USB flash drives?

This assessment helps identify what level of security protection is required. In the case of MAC 5, the answer to many of these questions is "yes" so the system is treated as a high security risk system. And we have put a large number of controls in place to ensure protection.



Software development maturity

By making security fundamental to everything we build, we can make products smarter and safer.

It starts with software engineers

Our talented software engineers are equipped with state-of-the-art software engineering tools and training focused on security. In addition, GE's central cybersecurity team is constantly monitoring for new threats, and uses this information to train the design staff.

A system of checks and balances

Using tools that look at the software our engineers create, we check for weaknesses that might leave the software vulnerable to cyber risks.

Next, the software is put through tests that simulate real-world threats. If any are found, we work to fix those issues.

Finally, our most senior design team members review the software at both the architecture level and at the implementation level. Even in the cyber world, there's still a need for human expertise.

Product security

Minimize the attack surface

A key principle is to minimize the parts of the system that are exposed to threats. In the case of MAC 5, all software services embedded in the operating system that are not explicitly needed to run the medical applications are removed or disabled. In short, fewer networking features mean fewer potential footholds for a would-be attacker.

Always updating

One of the simplest ways to keep a computer system secure is to make sure that the latest version of the operating system is installed. We continuously monitor for security issues and provide OS patches and software updates to make the MAC 5 one of the most safe and secure ECG systems on the market.

Only talk to things you recognize

MAC 5 uses a firewall to block unsolicited network traffic. MAC 5 owners can limit which network devices can connect, and can block devices that are unknown and potentially unsafe.

A smarter USB connection

MAC 5 protects itself against USB-borne attacks by allowing an administrator to enable/disable the use of USB ports. Running applications from USB flash drives is not allowed.

Maintaining patient data security

Protecting the systems against malware and other attacks is one part of system security, but it is also crucial to protect the patient information stored in that system.

Step 1: Patient data encryption

We encrypt all patient information stored on the MAC 5 using world-class encryption software.

Step 2: Username and password authentication

As an added layer of security, the MAC 5 offers the option to create a username and password.

Step 3: Secure network connections

MAC 5 uses a single sign-on known as LDAP. This allows users to get access to the system with the same login credentials they use for other hospital enterprise systems. In the MAC 5, LDAP is secure by default (LDAPS).

MAC 5 includes enterprise-grade wireless security to protect data in transit.

Security logging

MAC 5 monitors and records useful security-related activities. This includes user logins, network connections, and so on. In the unlikely event of a security breach, we can use this information to determine two important things:

- How did the breach occur, and what damage may have been done?
- How can a similar breach be prevented in future security updates to the system?

With this information, users can take full advantage of MAC 5's security features.

Ongoing security vigilance

As you can see, we've done a lot to make the MAC 5 secure, but the security world is always changing, so we have to stay vigilant.

Monitoring for new threats

One of the advantages of a big company like GE Healthcare is that we have a strong central security team that is constantly monitoring for new security threats. This central team is in regular communication with our electrocardiograph workstation designers, so the MAC 5 design team can make additional security patches to address vulnerabilities as needed.

Disaster recovery plan

MAC 5 has a security logging system that can be very helpful when recovering from a security breach. We can use this data to help understand the nature of the breach and the damage done. It's important for you and your staff also to have a disaster prevention and recovery plan. Consider these things when making your plan:

- Secure your electrocardiograph workstation system with non-default usernames and passwords. For rapid access to the MAC 5 you may elect to configure it with limited security protections. This flexibility allows you to tailor the level of security to meet your specific needs.
- Have good physical control over your system. In some cases, this means storing the system in a limited access area so that unauthorized users cannot attempt to use the system.
- Set up your system to send ECGs and patient information to your MUSE™ system or EMR immediately after every exam, and erase local copies. This will ensure that you can protect patient data in one place instead of two.
- Save MAC 5 configuration settings to backup media to facilitate quicker setup of additional MAC 5 systems.

Customer communication

Cybersecurity and data privacy is a team sport. When MAC 5 owners and MAC 5 designers work together, we can make sure that we are doing everything we can to stop security threats.

The MAC 5 owners and designers communication plan

Privacy and Security Manual

We publish the technical details of our security elements as part of the MAC 5 user manual and service documentation. Contact your local GE representative if a copy is needed.

MDS2 form

The MDS2 questionnaire provides answers to a list of standard security questions that are important to cybersecurity experts and is used across the industry. MAC 5 version is available upon request.

JB18565XX