



Your  
**CYBERSECURITY**  
is our priority.

Committed to keeping  
healthcare information secure

# We live in a dangerous world

Gone are the days when cyber threats would single out specific individuals, government entities and financial institutions. In today's digital era, the healthcare industry finds itself increasingly at the heart of these attacks.

Whether unintentional – such as the credit card details stealing Zotob Worm virus which found its way into a NICU's fetal heart monitors – or intentional, like a ransomware attack that shutdown a Los Angeles hospital's computers, forcing patients to seek treatment elsewhere, these threats are very real and do not discriminate.

At Dräger, we recognise that maintaining a secure network is a team effort. Hospital IT administrators want to align with a medical device manufacturer that will be their partner. The more security that is already built into a medical device, system or solution, the easier the purchasing decision becomes.

*Your cybersecurity is our priority.*



## WHAT IS CYBERSECURITY?

Cybersecurity is an ongoing process that encompasses procedures, policies, software and hardware. It's the measures taken to protect assets and economic activities from threats through the protection of information.

Threats attack assets – whether it's a medical device or entire institution – by targeting vulnerabilities which could impact your patients' care.

As a result, hospitals may face exposure to the following risks:

- Patient safety (injury, fatality)
- Production, equipment and financial loss
- Loss of sensitive hospital and/or patient data

At Dräger, we realise the importance of testing and continually updating security requirements for our existing portfolio. We've also identified that security vulnerabilities must now be considered during the planning/design and development cycles of all future product development.

**“Dräger’s commitment to improving healthcare cybersecurity is an excellent example that other device manufacturers should follow.”**

- Billy Rios, Founder of Whitescope, LLC



## DRÄGER’S APPROACH

### Striking a Balance

A secure system for you starts with a secure device from us. We take into account each challenge and concern related to:

- Device usability, complexity & lifecycle
- Patient safety
- Non-compatible internal IT controls
- Conflicting priorities of stakeholders
- Medical staff
  - Biomed
  - Hospital IT
  - Patient
  - Regulatory

and marry it with security.

### Laying Our Cybersecurity Groundwork

We understand the gravity of these attacks, which is why we’ve proactively:

- Established a dedicated cybersecurity team
- Developed a coordinated disclosure statement to act as a single point of contact for security issues
- Provided security training employees involved with Development Lifecycle
- Certain Dräger medical devices, including patient monitoring and anaesthesia, are being processed by the Defense Health Agency for U.S. Department of Defense Risk Management Framework (RMF) Certification.\*

### Partnering with Security Industry Experts

Our work with leaders in the cybersecurity field allows us to equip our devices, and ultimately you, with the advanced protection for your patients. From penetration testing to secure coding training to threat analysis and security training, our security consultants have their fingers on the pulse of the industry.

### Delivering Secure Solutions

Just like the challenge of breaking a code fuels hackers, we’re driven by providing your patient, your team and your hospital with secure solutions. Constant innovation ensures we deliver medical solutions you can trust. That’s why we’re:

- Implementing effective product security elements into our development process<sup>\*\*</sup>:
  - Security and privacy risk assessment
  - Threat analysis
  - Vulnerability testing
  - Independent penetration testing
- Updating products appropriately to comply with FDA and other regulatory agency guidance for cybersecurity including state-of-the-art encryption and authentication\*

\* Please ask your local Dräger representative for detailed information.

\*\* Implementation into product development in process. Not or not fully applied to legacy products.

#### CORPORATE HEADQUARTERS

Drägerwerk AG & Co. KGaA  
Moislinger Allee 53–55  
23558 Lübeck, Germany

[www.draeger.com](http://www.draeger.com)

#### Manufacturer:

Drägerwerk AG & Co. KGaA  
Moislinger Allee 53–55  
23542 Lübeck, Germany

Locate your Regional Sales  
Representative at:  
[www.draeger.com/contact](http://www.draeger.com/contact)



#### REGION DACH

Drägerwerk AG & Co. KGaA  
Moislinger Allee 53–55  
23558 Lübeck, Germany  
Tel +49 451 882 0  
Fax +49 451 882 2080  
[info@draeger.com](mailto:info@draeger.com)

#### REGION EUROPE

Drägerwerk AG & Co. KGaA  
Moislinger Allee 53–55  
23558 Lübeck, Germany  
Tel +49 451 882 0  
Fax +49 451 882 2080  
[info@draeger.com](mailto:info@draeger.com)

#### REGION MIDDLE EAST, AFRICA

Drägerwerk AG & Co. KGaA  
Branch Office  
P.O. Box 505108  
Dubai, United Arab Emirates  
Tel +971 4 4294 600  
Fax +971 4 4294 699  
[contactuae@draeger.com](mailto:contactuae@draeger.com)

#### REGION ASIA PACIFIC

Draeger Singapore Pte. Ltd.  
61 Science Park Road  
The Galen #04-01  
Singapore 117525  
Tel +65 6872 9288  
Fax +65 6259 0398  
[asia.pacific@draeger.com](mailto:asia.pacific@draeger.com)

#### REGION CENTRAL AND SOUTH AMERICA

Draeger Panamá Comercial  
S. de R.L.  
59 East Street, Nuevo Paitilla,  
House 31, San Francisco Town  
Panama City, Panama  
Tel +507 377-9100 / Fax -9130  
[servicioalcliente@draeger.com](mailto:servicioalcliente@draeger.com)