11TH eHEALTH SECURITY CONFERENCE

October 7th, 2026

Meet the presenters

Edward Moore

Partner - Deloitte Spain

EMEA Life Science & Health Care Cyber Lead at Deloitte, leading a 180-member team delivering managed security services and driving global collaboration and innovation in life sciences and health care cybersecurity.

Yiannis Ioannides

Partner - Deloitte Cyprus

Yiannis is a leading the Cyber Services of Deloitte Cyprus having over 15 years of experience. Yiannis is leading the team responsible for providing a number of cyber risk services including Penetration Testing and Vulnerability Assessments, physical security assessments, social engineering, security configuration reviews and third-party assurance reports

 | Copyright © 2026 Deloitte Limited. All rights reserved.

Defensive Security

Overview of key challenges and good practices for healthcare cybersecurity, focusing on medical products.

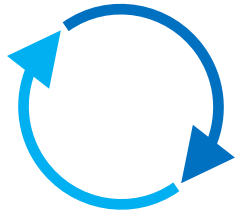
 | Copyright © 2026 Deloitte Limited. All rights reserved.

Threats and Challenges

Threats and challenges require robust cybersecurity measures.

Threats

- Ransomware & hacking, disruption of care/service
- Deception of staff through spoof email
- Unintentional or intentional 'Insider threat'
- Loss of patient information
- Data breach, information exfiltration and loss of assets
- Blackmail, extortion and duress through exploitation of exfiltrated sensitive data
- Software flaws, design defects, etc.



Challenges

- Medical devices are strictly regulated
- Modifications require manufacturer approval and validation.
- Operating system upgrades may be impossible due to hardware or driver dependencies.
- Security patches and updates must be assessed and approved by the manufacturer before implementation.
- Devices may be unsupported by the manufacturer but still in clinical use.

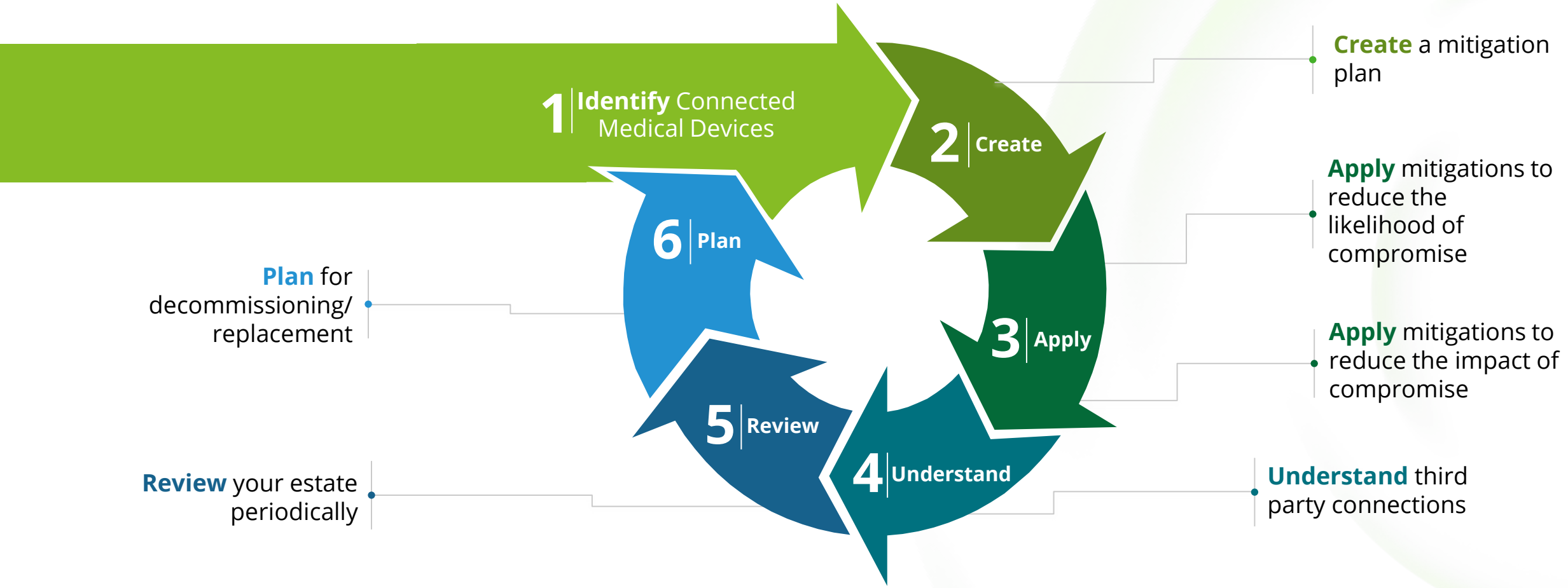
Implications

- Robust cybersecurity practices differentiate businesses and attract customers
- Increased vulnerability exposure
- Higher attack surface on clinical networks
- Likelihood of high-impact security incidents

 | Copyright © 2026 Deloitte Limited. All rights reserved.

Essential Security Lifecycle for Network-Connected Medical Devices

A step-by-step framework to identify, protect, and manage medical devices across their entire lifecycle.

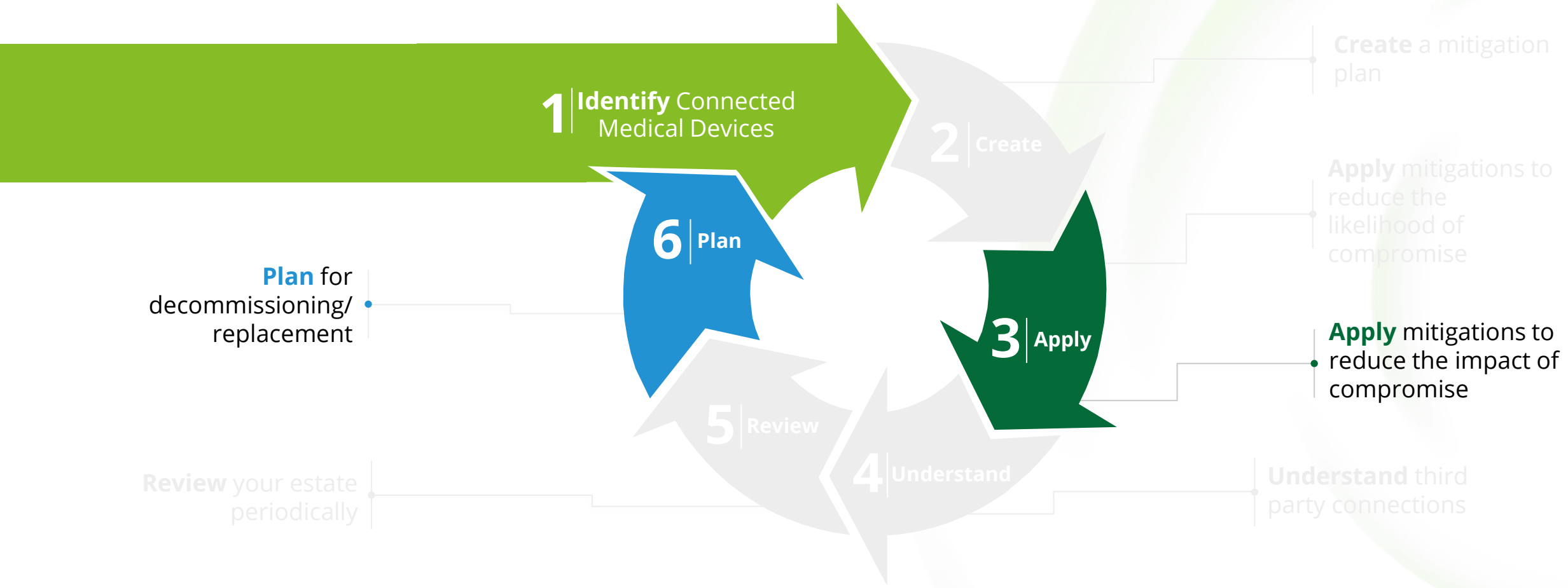


We review the steps that should apply to any network connected medical device regardless of operating systems.

 | Copyright © 2026 Deloitte Limited. All rights reserved.

Essential Security Lifecycle for Network-Connected Medical Devices

A step-by-step framework to identify, protect, and manage medical devices across their entire lifecycle.



We review the steps that should apply to any network connected medical device regardless of operating systems.

 | Copyright © 2026 Deloitte Limited. All rights reserved.

Security guidance on protecting medical devices

Identify Connected Medical Devices.

Identify all the devices within your estate that are within scope and out of scope and create a complete network topology

- Operating System
- Software
- Version
- Ports / protocols
- Application services utilized
- Store / transmit personal data?

What if you don't know what devices you have within your estate?

 | Copyright © 2026 Deloitte Limited. All rights reserved.

Security guidance on protecting medical devices

Apply mitigations to reduce the impact of compromise.

An **unpatched end user device** that is directly exposed to malicious content is likely to result in successful compromise. The **impact of compromise** can be reduced by controlling **access to enterprise services** hosting sensitive data and **improving the ability to detect** attacks.

- Remove access to services
- Network zoning
- Protective monitoring capability improvement including pentesting
- Anti-malware and intrusion detection products
- Incident response
- Raise Awareness with clinical colleagues

We recommend to include a compromised medical device as part of your regular incident response exercises.

 | Copyright © 2026 Deloitte Limited. All rights reserved.

Security guidance on protecting medical devices

Plan to periodically review your estate for decommissioning/replacement of devices.

Asset inventory

Estate Management

Implement a system or technology to track, manage, and monitor medical equipment and devices throughout their lifecycle to ensure safety, regulatory compliance, and operational

Plan

Decommission plan

This will ensure safe, efficient management of equipment throughout its lifecycle by detailing the process for removing devices from service and properly disposing of them.

Life expectancy of a device

Estate Management

Life expectancy should be factored into the original procurement so that replacement time-scales and costs can be understood.

.

Patient data

Estate Management

Data should be forensically erased. Any data stored on a connected medical device should be sanitised prior to disposal and before the device leaves the organization

 | Copyright © 2026 Deloitte Limited. All rights reserved.

Crisis Management In Healthcare

From public health emergencies to cyber incidents and operational failures, healthcare institutions must be prepared to respond quickly, coordinate effectively, and recover with resilience.

 | Copyright © 2026 Deloitte Limited. All rights reserved.

Crisis readiness protects patients, staff, and healthcare trust

Strong crisis response preserves care delivery, workforce resilience, compliance, and public confidence

Why It Matters

1. Preserve patient safety in emergencies
2. Ensure continuity of essential care
3. Protect staff wellbeing and capacity
4. Maintain regulatory compliance under pressure
5. Sustain public trust and credibility
6. Reduce harm from delayed decisions

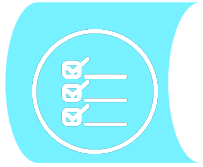
Patient Safety

Core priorities during healthcare emergencies

Prioritize critical patients and services

Protect staffing and clinical handoffs

Coordinate rapid escalation and communication



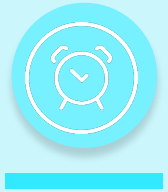
Document actions for compliance and trust

| Copyright © 2026 Deloitte Limited. All rights reserved.

Healthcare organizations must prepare for four major crisis categories

From outbreaks to cyberattacks, crises can rapidly disrupt care delivery and safety

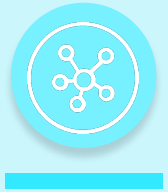
Cyber Incidents



Cyber incidents compromise patient data, digital workflows, and critical communications infrastructure.

Ransomware, data breaches, and system outages can halt clinical and administrative operations.

Disease Outbreaks



Infectious outbreaks spread quickly and strain isolation protocols, surge planning, and supplies.

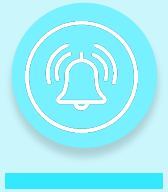
PPE, medicine, blood, and staffing shortages reduce capacity and delay treatment.

Infrastructure Failures

Infrastructure failures threaten facility operations, clinical continuity, and patient safety across departments.

Power loss, equipment failure, or utility disruption can force evacuation or service diversion.

External Crises



Mass casualty events and reputational crises create sudden operational, legal, and media pressure.

High-profile incidents and public criticism can damage trust, funding, and stakeholder confidence.

| Copyright © 2026 Deloitte Limited. All rights reserved.

A structured crisis cycle strengthens readiness, response, and resilience

Eight connected actions create a continuous loop of healthcare crisis readiness and improvement.

Track conditions, indicators, and lessons continuously to strengthen future readiness and resilience.

Reduce crisis likelihood through controls, safeguards, maintenance, and policy-driven risk mitigation.

Restore services, sustain critical operations, and support safe return to normal performance.

Identify priority threats, vulnerable operations, and likely impacts across clinical and business functions.

Stabilize the situation, protect patients and staff, and limit operational disruption.

Define roles, playbooks, training, and resources needed for coordinated crisis response.

Mobilize command structures, communications, and response teams once crisis thresholds are reached.

Detect emerging incidents quickly through alerts, surveillance, escalation protocols, and frontline reporting.

| Copyright © 2026 Deloitte Limited. All rights reserved.

Four practical actions strengthen crisis response across teams and operations

Define roles, communicate clearly, rehearse response, and learn quickly after every incident.

Clarify Roles

Define decision rights, responsibilities, and escalation protocols so leaders and frontline teams can act quickly without confusion.

Strengthen Communications

Use clear channels, message templates, and status updates to coordinate teams, inform stakeholders, and reduce misinformation.

Rehearse Continuity

Run drills regularly and maintain business continuity plans to test readiness, sustain operations, and expose response gaps.

Review and Improve

Conduct after-action reviews, capture lessons, assign improvements, and update plans, training, and protocols after each event.

| Copyright © 2026 Deloitte Limited. All rights reserved.

Thank you!

Q&A

 | Copyright © 2026 Deloitte Limited. All rights reserved.