



SAFHE 2026

SOUTHERN AFRICAN
HEALTHCARE CONFERENCE

SYNERGY
IN ACTION:

SHAPING THE FUTURE OF
HEALTHCARE TOGETHER



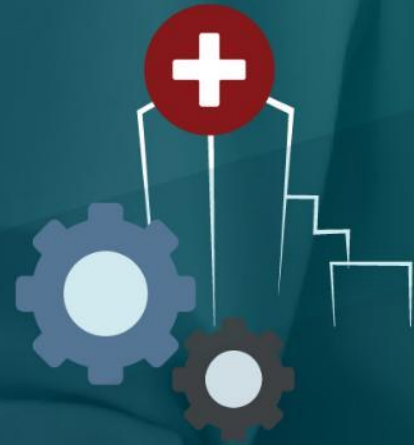
9 – 10 JUNE 2026



CTICC 2 CAPE TOWN

CYBERSECURITY MANAGEMENT OF MEDICAL DEVICES

Van Heerden Fourie



SAFHE 2026

SOUTHERN AFRICAN
HEALTHCARE CONFERENCE

SYNERGY
IN ACTION: SHAPING THE FUTURE OF
HEALTHCARE TOGETHER



9 – 10 JUNE 2026



CTICC 2 CAPE TOWN

Cybersecurity management of medical devices

Van Heerden Fourie

IN THIS PRESENTATION

1

Introduction

2

Staff
Development

3

Equipment
Life cycle

4

Incident
Response

5

Conclusion

INTRODUCTION



CYBERSECURITY STATISTICS

- Hospitals = 17% of ransomware attacks
- 53% of networked medical devices critical vulnerability
- 21% of medical devices secured by weak/default credentials
- 14% of connected medical devices - unsupported OS
- 6.2 vulnerabilities per medical device
- \$7.42 million – average cost per data breach
- 100 Million+ individuals affected
- Media announcements = ↑network penetration attempts
- Local supply chain affected





WHY TARGET HEALTHCARE?

- Irreplaceable sensitive data
- Complex aged infrastructure
- Distributed users
- Time-critical workflows
- Third party dependencies
- Down-time becomes operational harm
- \$1000/record on dark web





CYBERSECURITY: THINGS TO CONSIDER

- **Organisational Information Security Management System (ISMS)**
 - Norms & Standards
 - Network Infrastructure
 - Technology
- **Budgetary provision**
- **Skilled resources**
- **Equipment life cycle**



STAFF DEVELOPMENT



STAFF DEVELOPMENT

Hospital Staff:

- Awareness training
- Simulations e.g. Simulated Phishing

Technical Staff:

- Continuous Self Development
- Network / Cybersecurity basics
- Collaboration



EQUIPMENT LIFE CYCLE



EQUIPMENT LIFE CYCLE

1. Capital Procurement
2. Asset Management
3. Maintenance
4. Data Privacy





CAPITAL PROCUREMENT

1. Entrance point
2. Cybersecurity specifications
3. Standard disclosure templates
(e.g MDS2)
4. Regulatory approvals
5. NDA & SLA





ASSET MANAGEMENT

1. Insufficient Attribute Detail
2. System limitations
3. Network information
4. New opportunities
5. Detailed information from network
6. Manual asset counts still required?





MAINTENANCE

Planned Maintenance

Time & Material

Wear & Tear

Sensors

Calibration

Software Maintenance

Periodic application SW updates

Operating system upgrades

Security updates





DATA PRIVACY

Internal non-disclosure agreements (NDA)

NDA's with service agents

Patient data on faulty equipment

Decommissioning of medical equipment

Access Control

Physical Access Control

Logical Access Control

Access management software



INCIDENT RESPONSE



IMPORTANT FACTORS

Identify, Isolate & Remediate

Communication

Downtime – break in process flows

Usually requires a 're-image' of equipment

Potential information loss

Continuous improvement



CONCLUSION



TAKE-HOME MESSAGE

- Cybersecurity is a team sport
- Continuous professional development
- Improve asset life cycle processes
- Continuous improvement





SAFHE 2026

SOUTHERN AFRICAN
HEALTHCARE CONFERENCE

SYNERGY
IN ACTION:

SHAPING THE FUTURE OF
HEALTHCARE TOGETHER

Thank you / Q&A



REFERENCES AND LINKS

60 Healthcare and Medical Device Cybersecurity Risk Statistics for 2025 | C2A

Security - The Only Risk-Driven DevSecOps Platform

IoMT Vulnerabilities Statistics 2025: 99% of Hospitals Exposed

Claroty's State of CPS Security Report: Healthcare Exposures 2025 | Claroty

Medical Device Cybersecurity: Best Practices, FAQs, and Examples

Healthcare Cybersecurity Threat Report 2026-2027: Original Data & Actionable Insights

Healthcare Data Breaches 2025 Statistics: \$10.22M Cost

Medical device cyberattacks push hospitals into crisis mode - Help Net Security