Cybersecurity for medical devices

Standardization of medical device cyber security

Andreas Lämmerzahl, Executive Director R&D

Certified B Corporation

Life. Science.

DOSIMETRY

iba

NO STANDARD or REGULATION ENSURES YOUR DEVICE ~~IS~~ WILL BE CYBER-SAFE

Today

1. Cybersecurity & Situation in healthcare
2. Networked medical devices
   Safe = Secure?
3. Transparency & Standards

Cybersecurity

Definition

- Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats.

- A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks that aim to disable or disrupt a system's or device's operations.

From: https://www.techtarget.com/searchsecurity/definition/cybersecurity

Protection goals - CIA

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

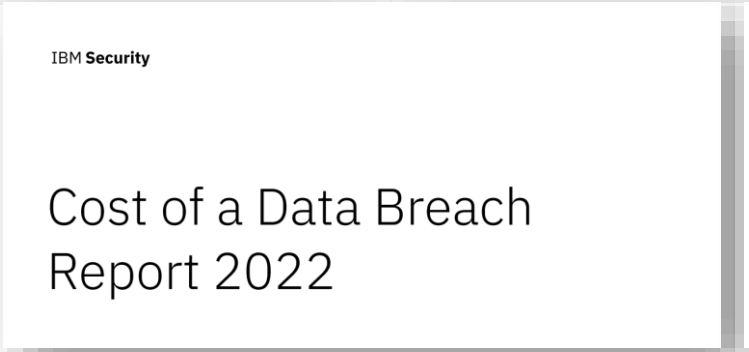
Of data, services and assets

- **Integrity →**
  - Authentic
  - Accurate
  - Reliable
  - Consistent

Cybersecurity situation in Healthcare

Cybersecurity situation in Healthcare

- Recent reports, mainly US driven:



Healthcare under attack

statista

Search Statistics

Prices & Access | Statistics | Reports | Insights NEW | Infographics | Services | Login

Internet › Cyber Crime & Security

Global number of data breaches with confirmed data loss from November 2020 to October 2021, by target industry and organization size

Search: Records: 13

Characteristic	Total	Small	Large	Unknown
Total	5,212	715	255	4,212
Finance	690	56	32	602
Professional	681	263	52	366
Unknown	651	1	3	647
Healthcare	571	14	10	547
Public administration	537	74	25	438
Information	378	27	10	341
Manufacturing	338	54	22	262
Education	282	57	15	210

Why is healthcare a top target?
→ High pressure

CommonSpirit Health confirms ransomware attack

Giles Bruce - Thursday, October 13th, 2022

Save Post Tweet Share Listen Text Size Print Email

After more than a week of IT outages at CommonSpirit Health hospitals across the country, the Chicago-based system confirmed it has fallen victim to a ransomware attack.

"Patients continue to receive the highest quality of care, and we are providing relevant updates on the ongoing situation to our patients, employees and caregivers," CommonSpirit said in an Oct. 12 statement. "Patient care remains our utmost priority and we apologize for any inconvenience this matter has created."

The ransomware attack has shut down EHRs and canceled appointments and surgeries at CommonSpirit hospitals from Washington to Texas to Tennessee. In one incident, the IT issues may have led a nurse in an already understaffed emergency room in Silverdale, Wash., to call 911 for help, the *Kitsap Sun* reported Oct. 12.

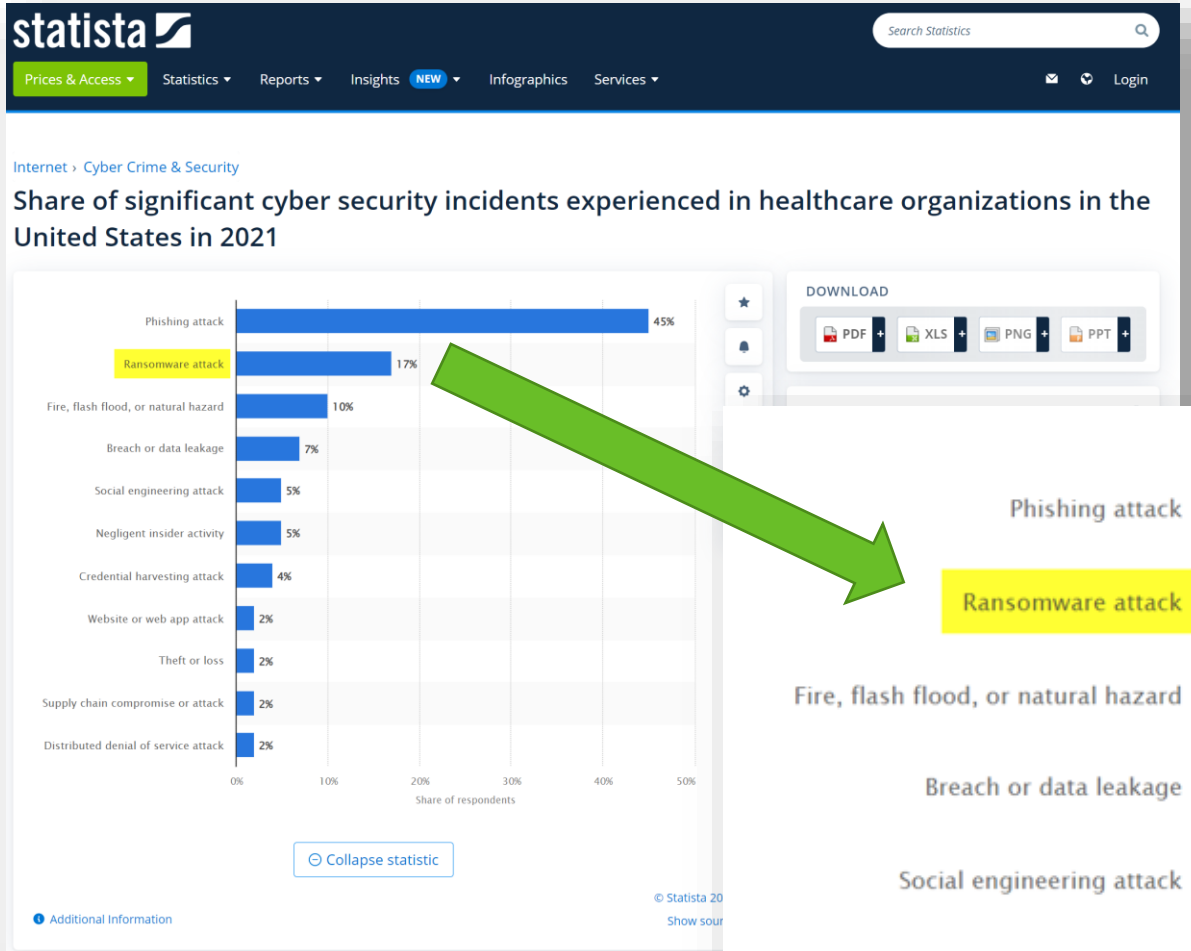
Healthcare under attack

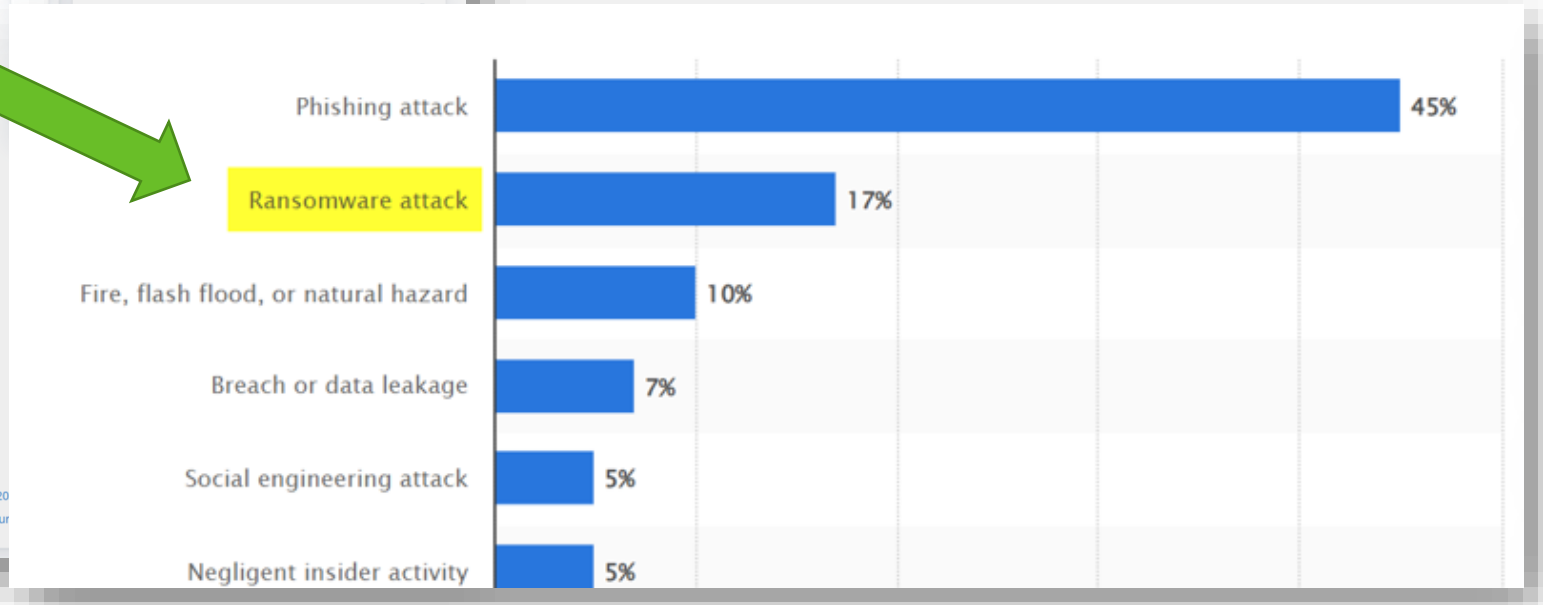
Industry	Average cost of data breach (USD millions)	
	2022	2021
Healthcare	9.23	10.1
Financial	5.72	5.97
Pharmaceuticals	5.04	5.01
Technology	4.88	4.97
Energy	4.65	4.72
…	…	…

Cost component	Average cost in 2022 (USD millions)
Notification	0.31
Post breach response	1.18
Detection and escalation	1.44
Lost business	1.42

Source: IBM Security, Cost of data breach report 2022

Ransomware is #2!





Some ransomware facts

Main Facts in healthcare	
66%	% of healthcare institutions hit by ransomware in 2021
61%	% of attacks resulting in data encryption

Trends in healthcare	
69%	Increase in volume of cyber attacks, highest across all sectors
67%	Increase in complexity of cyber attacks, highest across all sectors
59%	Increase in impact of cyber attacks, 2nd highest across all sectors

Consequences for hit healthcare institutions	
99%	% of institutions getting part of encrypted data back
65%	% of encrypted data restored after paying the ransom
14%	% of institutions using 3 methods in parallel to restore data- highest of all sectors
2%	%of institutions which paid the ransom and got ALL the data back

Source: *A Sophos Whitepaper. May 2022,* The State of Ransomware in Healthcare 2022

Some ransomware facts

Consequences for hit healthcare institutions	
65%	% of encrypted data restored after paying the ransom
14%	% of institutions using 3 methods in parallel to restore data- highest of all sectors

~~**What's your backup strategy?**~~

What's your recovery strategy?

How much time do you have for restore?

Networked medical devices

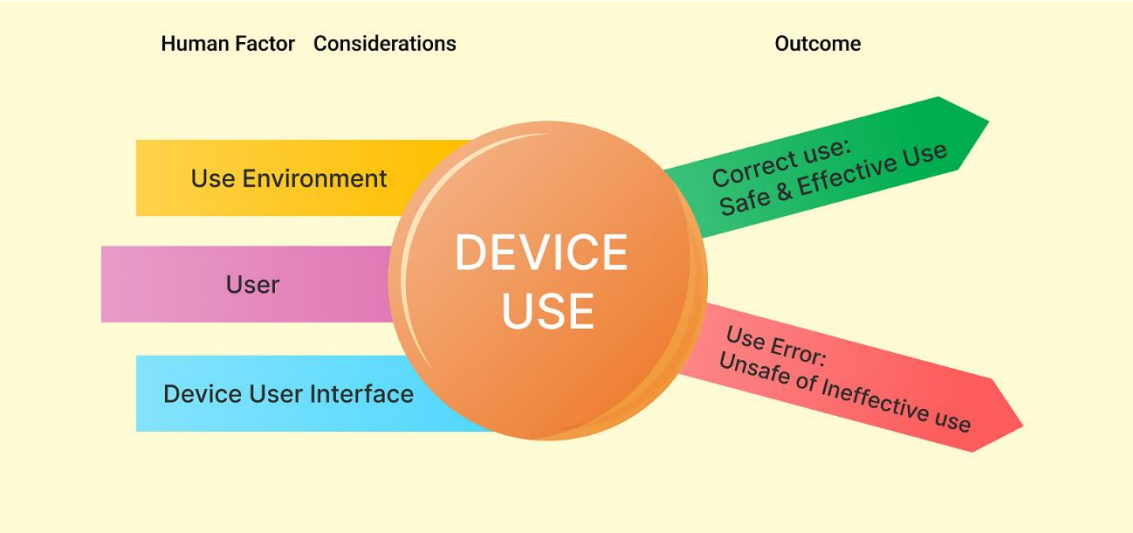
Safe Medical Devices

- A medical device is characterized by it's ***intended use***

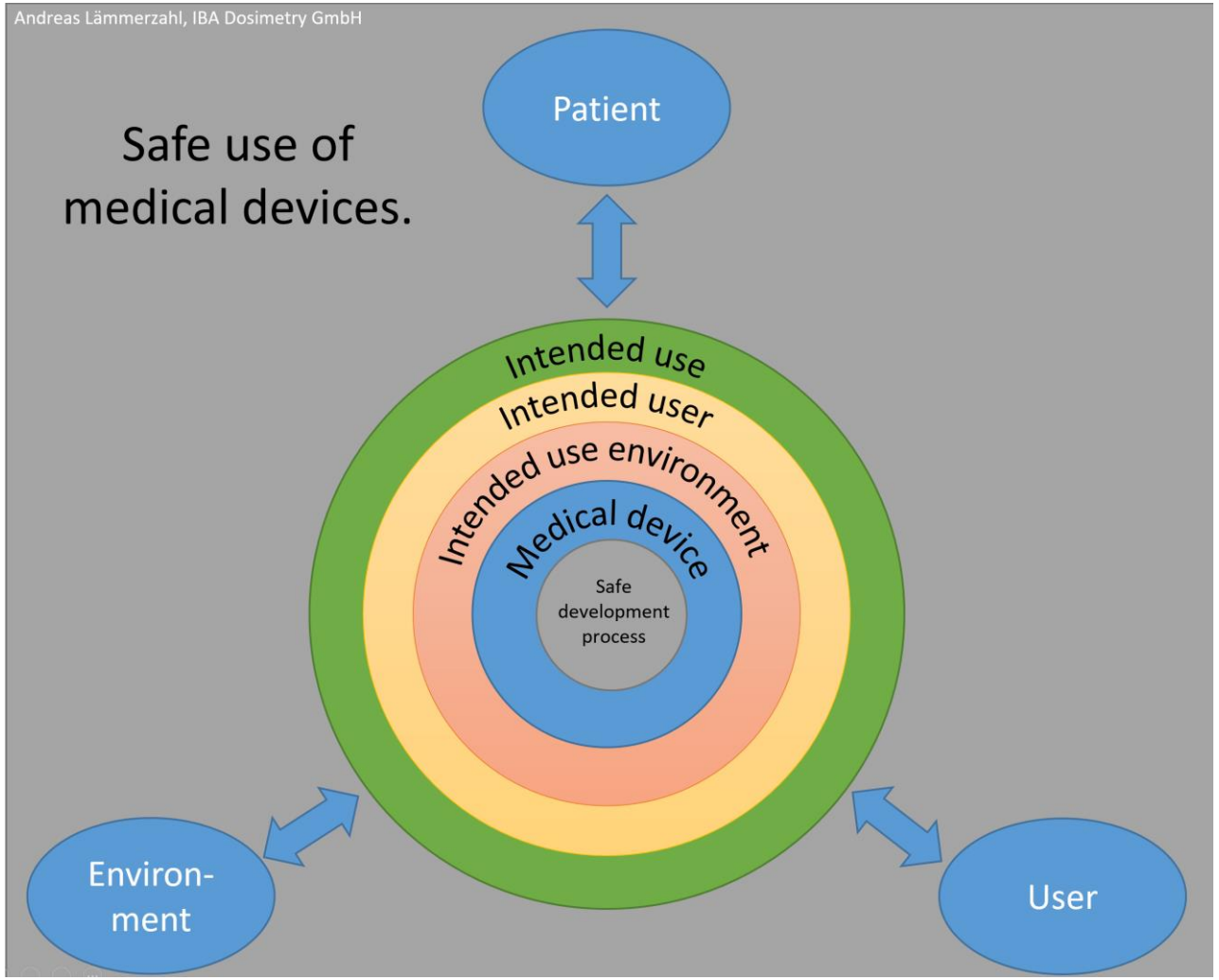
- The manufacturer ensures the ***safety / effectiveness*** respecting the intended use

- Safe use = minimizing the risk of harm to
  - Patients
  - Users
  - Environment
  - Property

- Product Risk management on manufacturer side

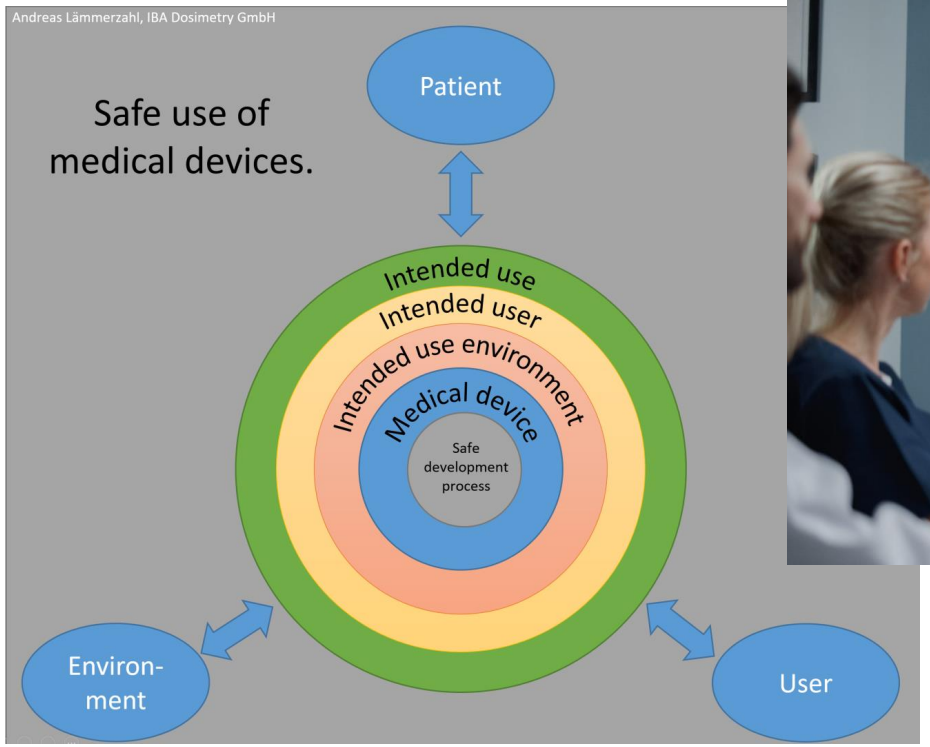


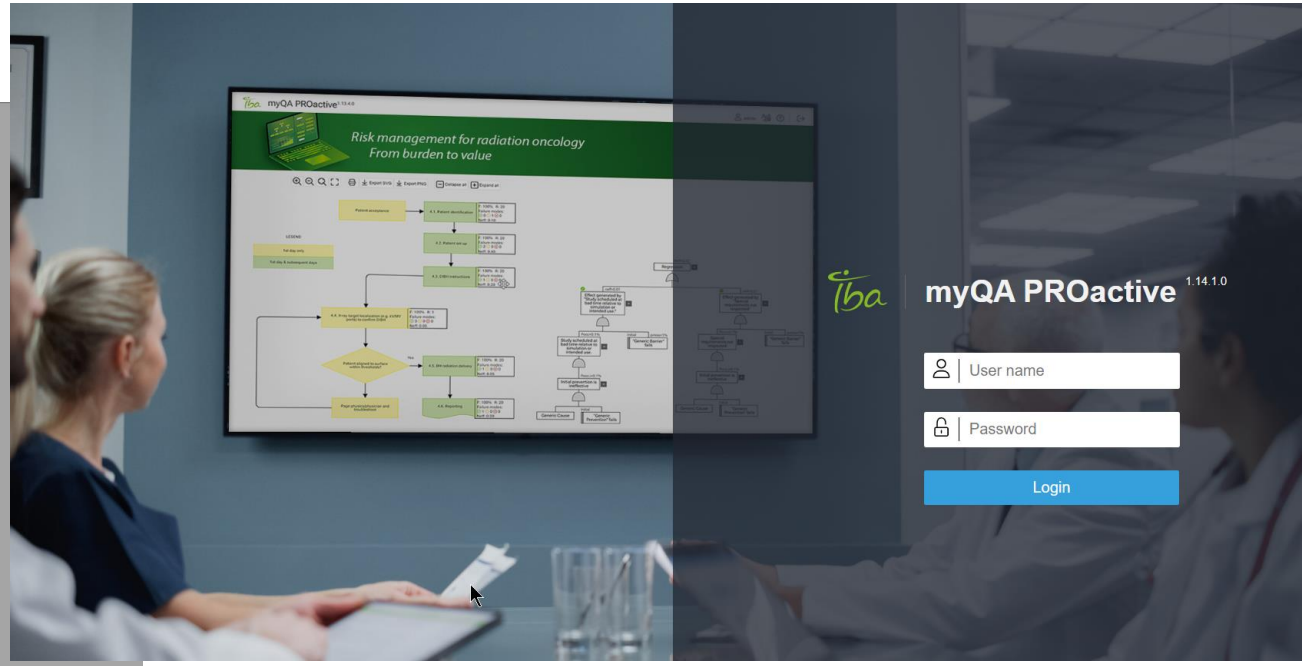
Safe use of medical devices



Clinical risk management

- Hospital specific interaction and interfaces in between intended use, use environment and intended user requires clinical risk management

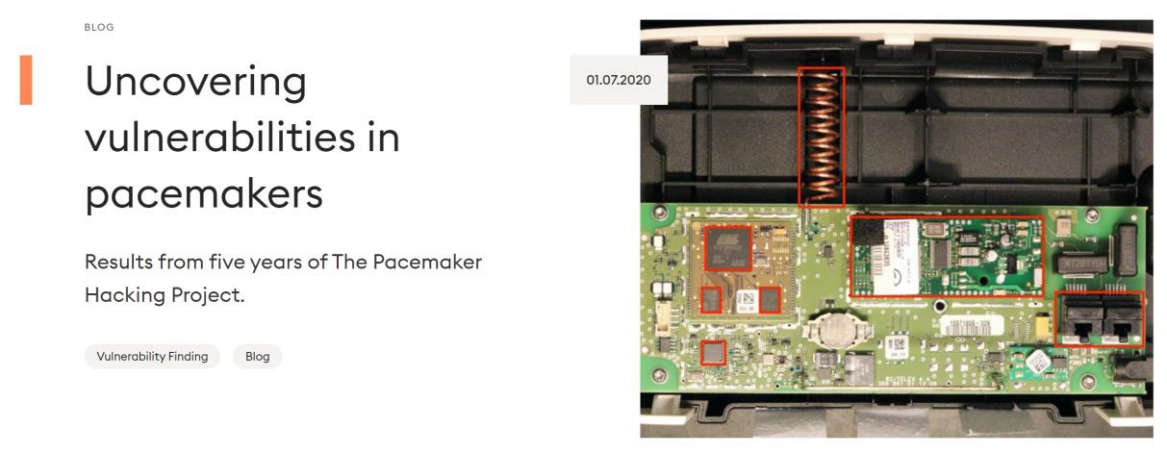




What is a networked medical device?

- Any medical device that communicates via networks or exchanges data via networks **or removable media**.
- **Not restricted to internet communication only**

- Wide range:
  - Health products
    (e. g. Bluetooth connected scale, watch)
  - heart pacemaker
  - infusion pumps
  - RT devices
  - remote controlled robotic surgery rooms
  - … and connected QA devices for RT …



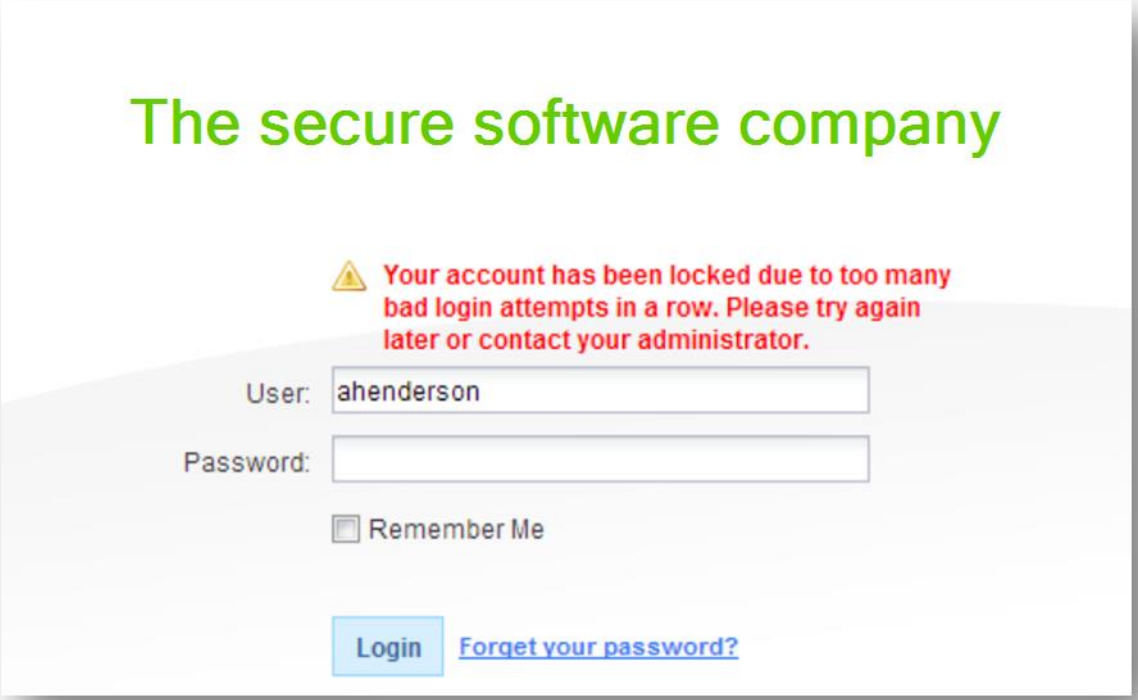
https://www.mnemonic.io/resources/blog/uncovering-vulnerabilities-in-pacemakers/

Safe = Secure?

The dilemma in standardization

Cyber security risk

- In principle, networked medical devices faces the same kind of attacks as any other networked system
- Any common measure applicable for networked systems shall be applicable for medical devices?

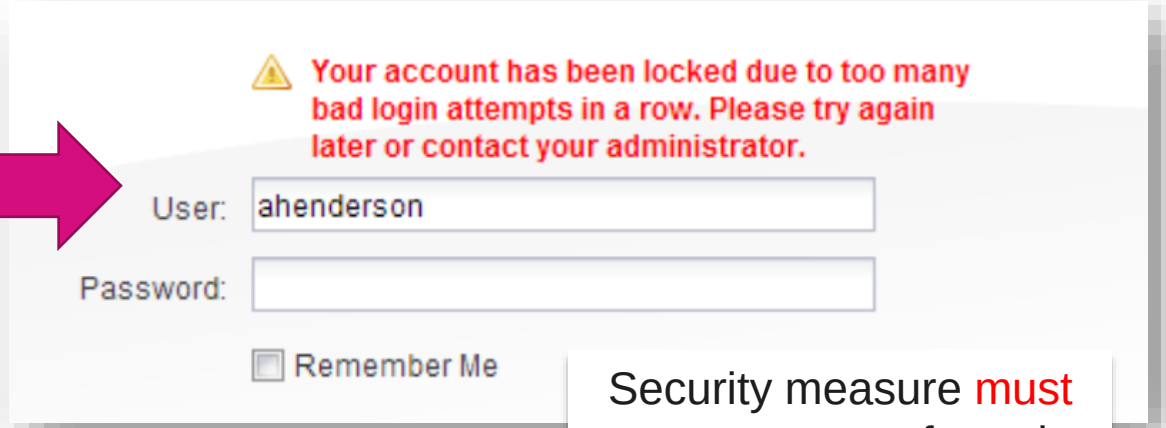


Security and safety ….

+

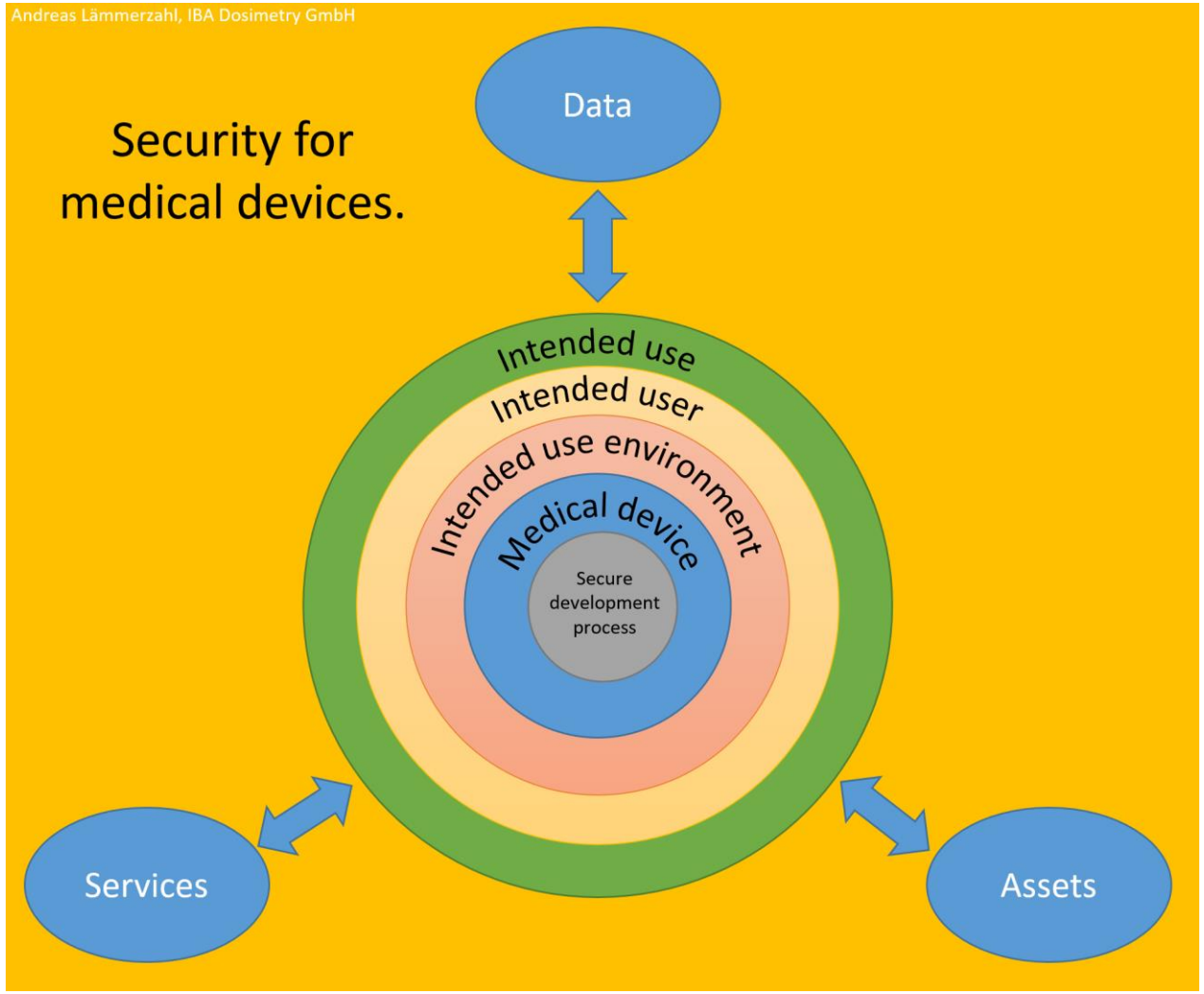
+

+



Security measure must not prevent safe and effective use

Always consider safety, intended use and context!



1. **Intended use**
2. **Safety**
3. **Cyber Security**

1. Cyber Security for safe and effective use
2. Cyber Security for assets / data privacy

Missing knowledge about highly complex intended use environment from security perspective and human factor

The dilemma

Safe Secure

The most important measure

Cybersecurity

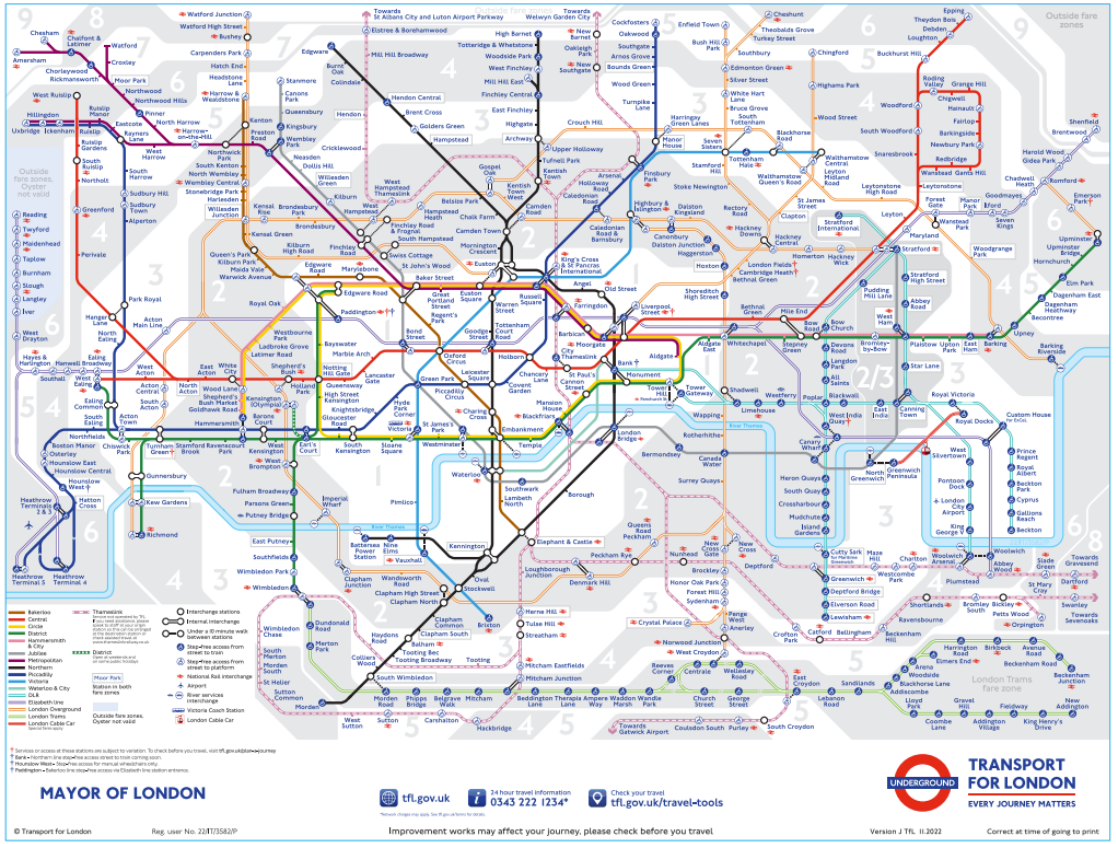
- Just safe cars don’t ensure safe traffic

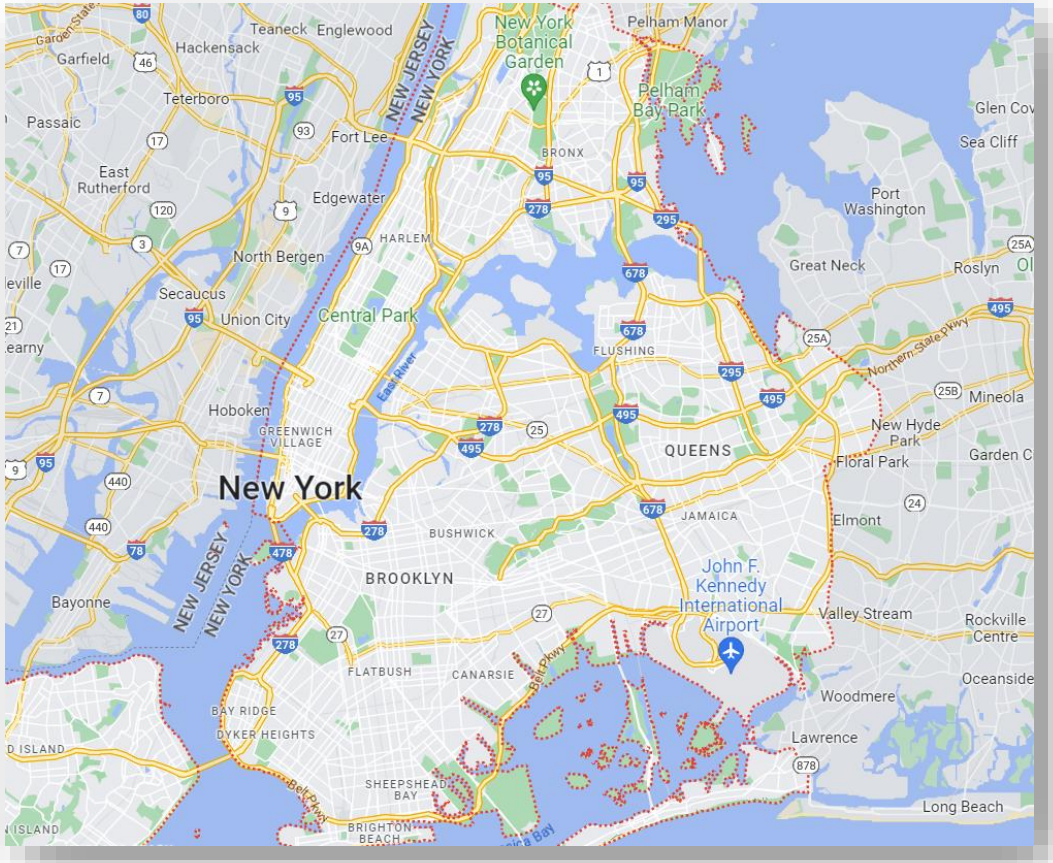
- A device cannot be ‘cyber-safe / secure’ without considering the use context
- An IT network cannot be ‘secure’ if the devices do not support a secure operation
- A pile of secure devices does not create a secure IT landscape

Cybersecurity

- London underground
  - Passengers → Data
  - Trains → Services, networked devices
  - Rails, tunnels → IT network
  - Traffic lights, signs and conductors → IT cybersecurity measures
  - Cybersecurity goal →
    - all passengers arrive safely at the right place
    - Trains don’t get stuck in tunnels

Transparency – key to Cybersecurity





MDS² - makes your AND manufacturers life easy

- **M**edical **D**evice **S**ecurity **M**anufacturer **D**isclosure **S**tatement

https://www.nema.org/Standards/view/Manufacturer-Disclosure-Statement-for-Medical-Device-Security

Manufacturer Disclosure Statement for Cyber Security			
IBA Dosimetry	myQA PROactive	accolade: P-21-008 ProActive	24-Feb-2023

- MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION
- AUTOMATIC LOGOFF (ALOF)
- AUDIT CONTROLS (AUDT)
- AUTHORIZATION (AUTH)
- CYBER SECURITY PRODUCT UPGRADES (CSUP)
- HEALTH DATA DE-IDENTIFICATION (DIDT)
- DATA BACKUP AND DISASTER RECOVERY (DTBK)
- EMERGENCY ACCESS (EMRG)
- HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)
- MALWARE DETECTION/PROTECTION (MLDP)
- NODE AUTHENTICATION (NAUT)
- CONNECTIVITY CAPABILITIES (CONN)
- PERSON AUTHENTICATION (PAUT)
- PHYSICAL LOCKS (PLOK)
- ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)
- SOFTWARE BILL OF MATERIALS (SBoM)
- SYSTEM AND APPLICATION HARDENING (SAHD)
- SECURITY GUIDANCE (SGUD)
- HEALTH DATA STORAGE CONFIDENTIALITY (STCF)
- TRANSMISSION CONFIDENTIALITY (TXCF)
- TRANSMISSION INTEGRITY (TXIG)
- REMOTE SERVICE (RMOT)
- OTHER SECURITY CONSIDERATIONS (OTHR)

Cybersecurity leaflet

myQA PROactive

CyberSecurity Leaflet

The purpose of this document is to describe the system for IT personnel to ensure secure and safe operations and use.

What is the system for?

- myQA PROactive implements prospective risk management in radiation oncology in a single, browser-based application that enables teams to structure, plan, execute and document risk management activities according to European regulations, state of the art international guidelines, and best practice worldwide.
- The system provides templates, tools, and guidance to:
  - Define, describe, visualize, and train clinical workflows and respective changes
  - Identify, assess, and manage potential risks
  - Visualize and analyze event causation chains
  - Develop and apply corrective measures
  - Compare effectiveness and costs of quality assurance scenarios
  - Implement the recommendations of AAPM Task Group 100

Standardization

How about standardization

- There are a lot of CS related standards for hospitals in EUROPE:
  - ISO 8001
  - ISO 27001 Series
  - NIST 2.0 …
- Medical device manufacturers MUST follow MDR (Medical Device Regulation) and several standards on how to develop safe medical devices
  - ISO 13485 (Quality Management) / ISO 14971 (Risk management)
  - DIN / EN 62304 & 82304 for Software Development Process
- ISO 27001, a guidance for implementation of CS management framework, also applicable, but not required for medical device manufacturers

What shall **manufacturers** do?

- Include cyber security aspects in device development
- Follow the processes (CE Mark) during development, including:
  - Penetration Tests
  - Provide proper documentation regarding CS
  - Cyber Security Risk Assessment
- Implement a vulnerability reporting & solution management
- Follow cyber security risk management in clinics

What shall **hospitals** do?

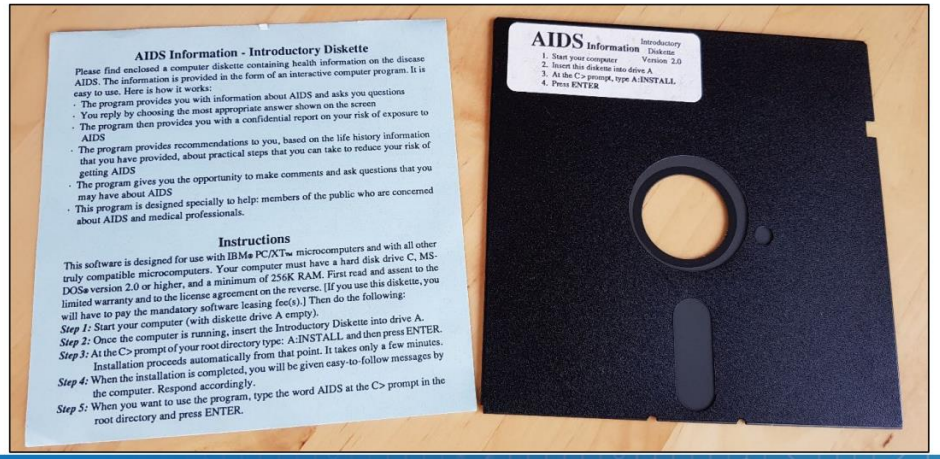
- Implement Cyber Security Risk Management
- Make sure, IT cyber security risk management is linked to clinical risk management
- Consider cyber security aspects even in purchasing process
- Be transparent towards the manufacturer
- Request from manufacturer:
  - MDS² form (be standardized)
  - Certification for cyber security management

Ransomware – 20.000 Floppy disks

The first ransomware attack

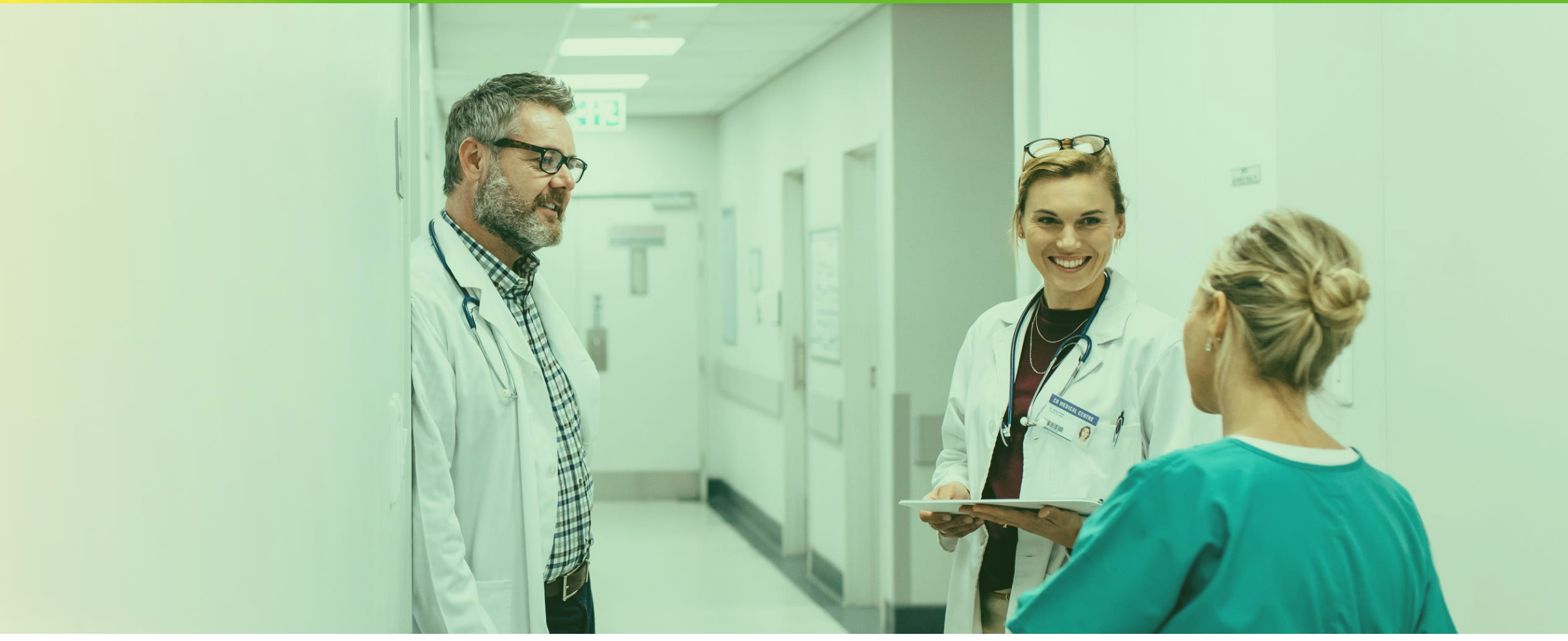
1989 PC Cyborg “AIDS Trojan”

- The first ransomware attack occurred in 1989 and had a healthcare theme
  - Biologist Joseph Popp distributed 20,000 floppy disks at the World Health Organization AIDS conference in Stockholm in 1989.
  - The trojanized disks would install malicious code to track reboots, display ransom demand after 90 reboots on a victim system that would count reboots. After 90 reboots, the system would display a message claiming to be from 'PC Cyborg Corporation' which said their software lease had expired and that they needed to send $189 to an address in Panama to regain access to their system.
  - Popp was eventually charged with blackmail but was later declared mentally unfit to stand trial.



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY
4

Source: HHS Cybersecurity Program, Health Sector Cybersecurity: 2021 Retrospective and 2022 Look Ahead



Andreas Lämmerzahl, Exec. Director R&D

Certified B Corporation

Life. Science.

iba