I am The Cavalry

Unpatchable

Living with a vulnerable implanted device

Marie Moe, PhD, Research Scientist at SINTEF

@MarieGMoe

@SINTEF_Infosec

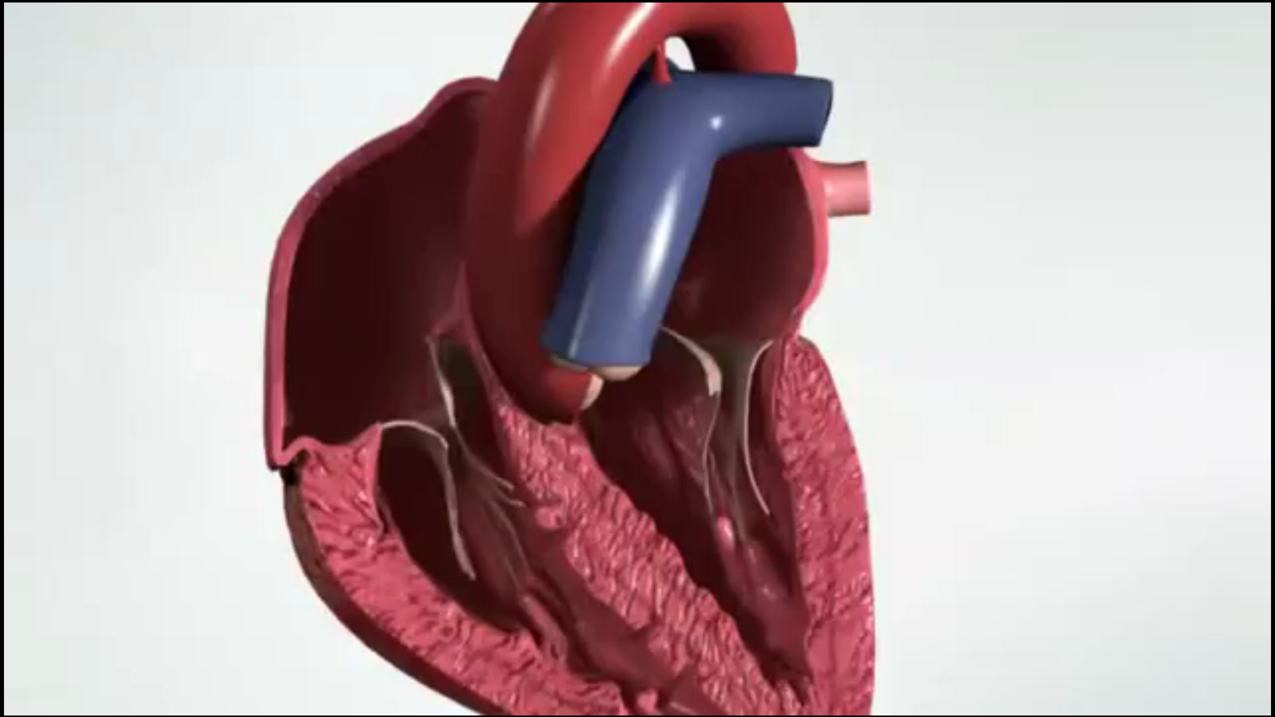
SINTEF

TROOPERS

Hack to save lives!

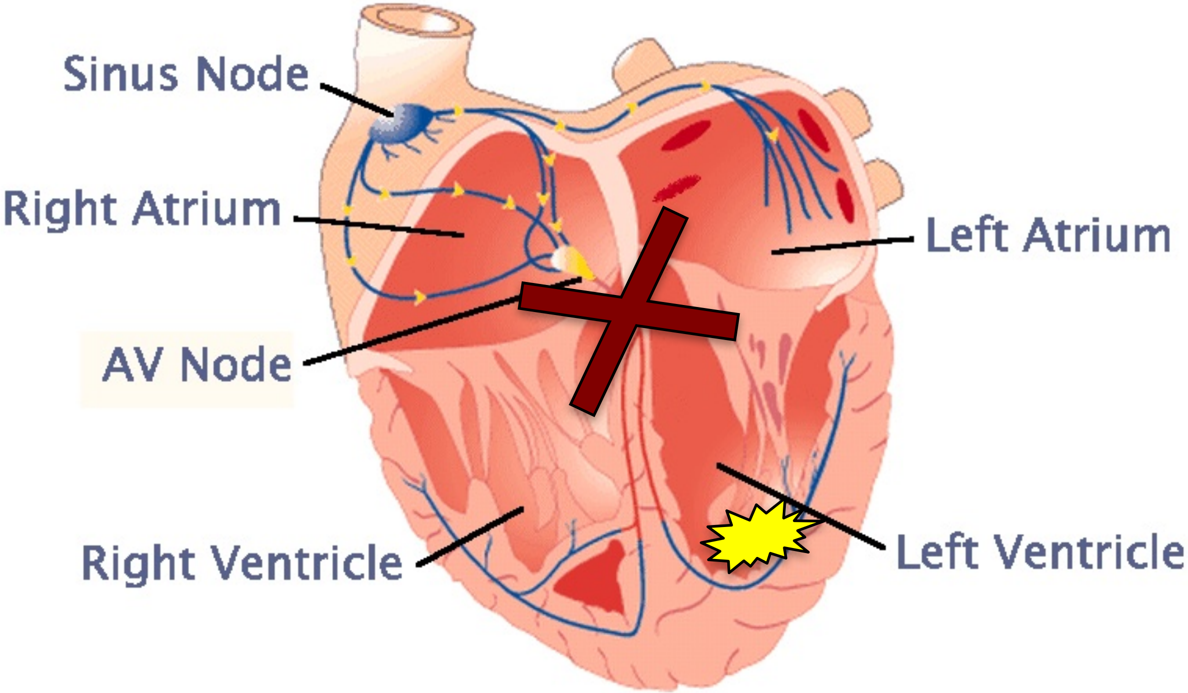
SINTEF

How the heart works



https://www.youtube.com/watch?v=d6RbN5lPqIU

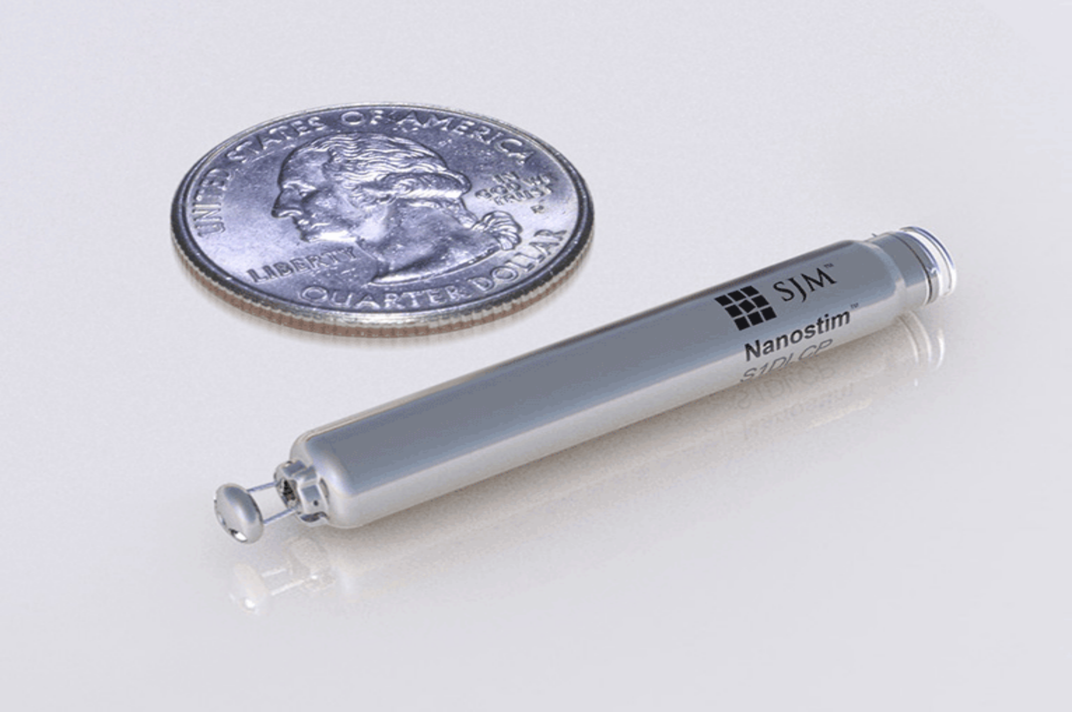
Electrical system of the heart



Pacemaker

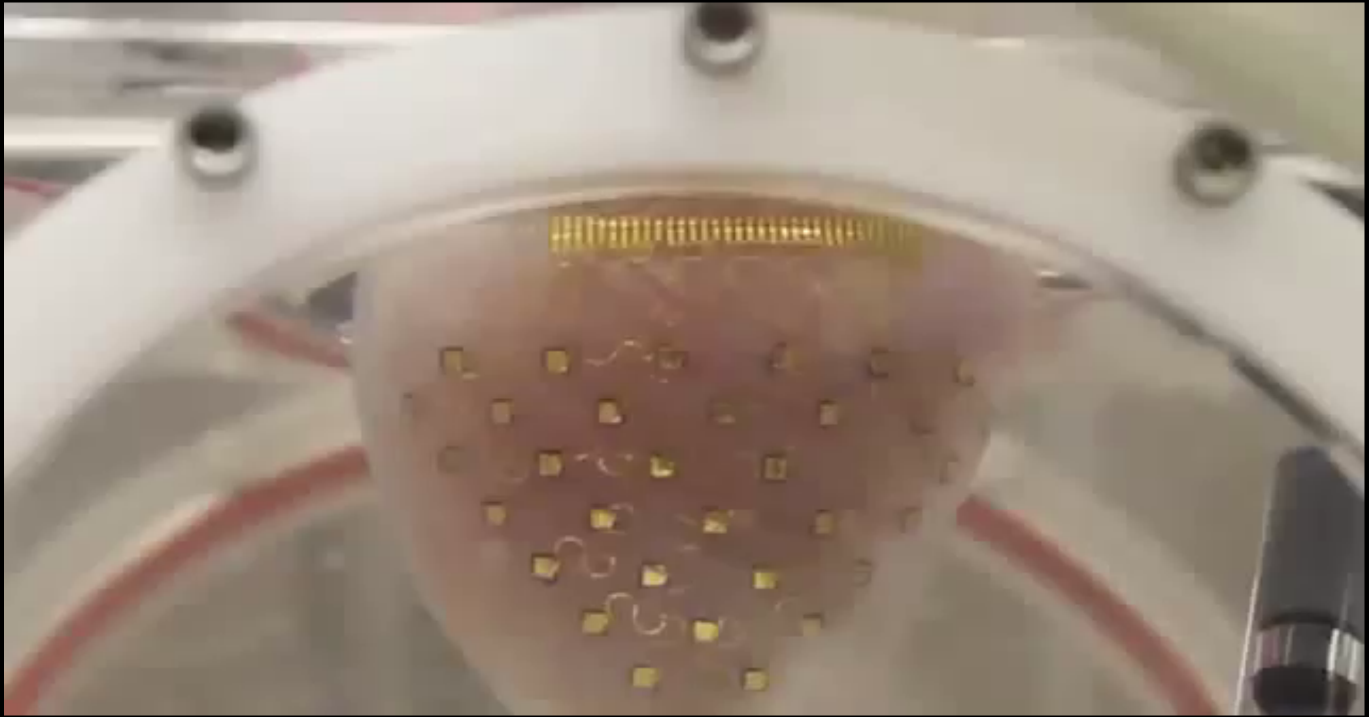
https://www.youtube.com/watch?v=-f2FKmMneXY

Leadless pacemaker



SINTEF

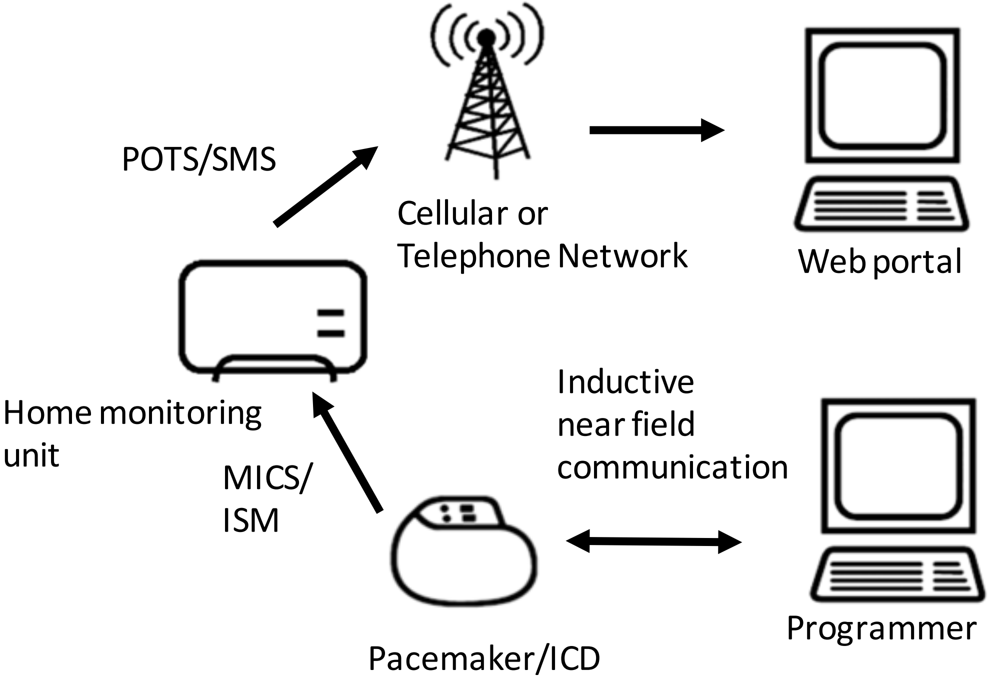
The future?



SINTEF

The Internet of Medical ”Things” is real,
and my heart is wired into it…

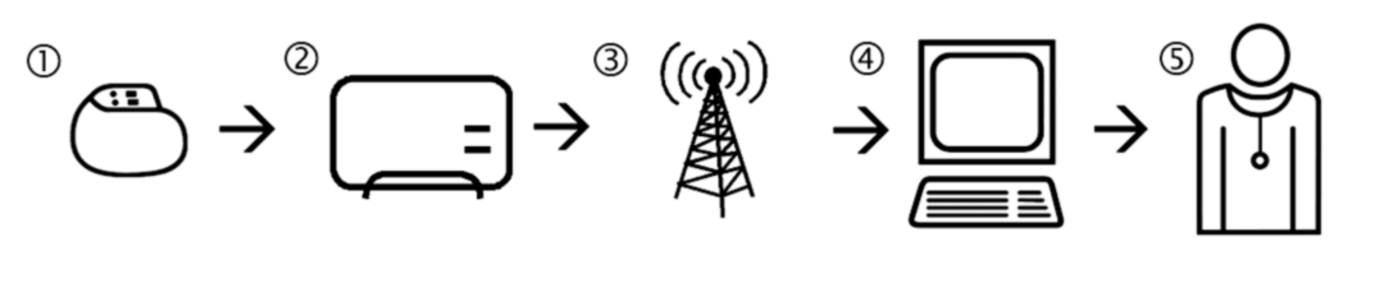
Remote monitoring



With connectivity comes vulnerability…

Potential threats

- Device is vulnerable?
- Access point is vulnerable?
- Mobile network is compromised?
- Server at vendor is compromised?
- Web site that doctor logs in to is vulnerable?



Potential impact

- Patient privacy issues
- Battery exhaustion
- Device malfunction
- Death threats and extortion
- Remote assassination scenario…

SINTEF

Personal Infrastructure

Your reliance on an infrastructure is inversely proportional to how invisible it is to you.

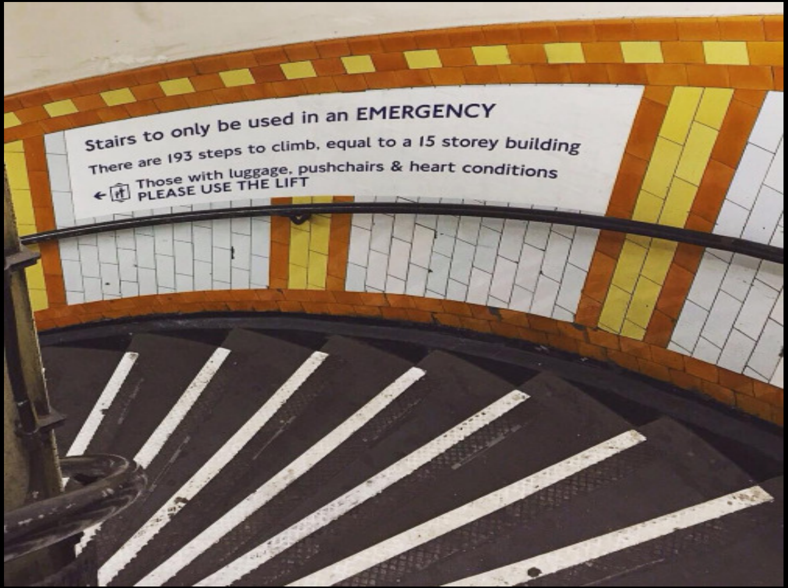
We all rely on oxygen, our lungs, and our hearts, but how often to we think about them?

How often do we do maintenance or debug them?

“Tech is not neutral nor value-free.”

Ben Zevenbergen, Troopers16

The stairs that almost killed me


Stairs to only be used in an EMERGENCY
There are 193 steps to climb, equal to a 15 storey building
Those with luggage, pushchairs & heart conditions
PLEASE USE THE LIFT

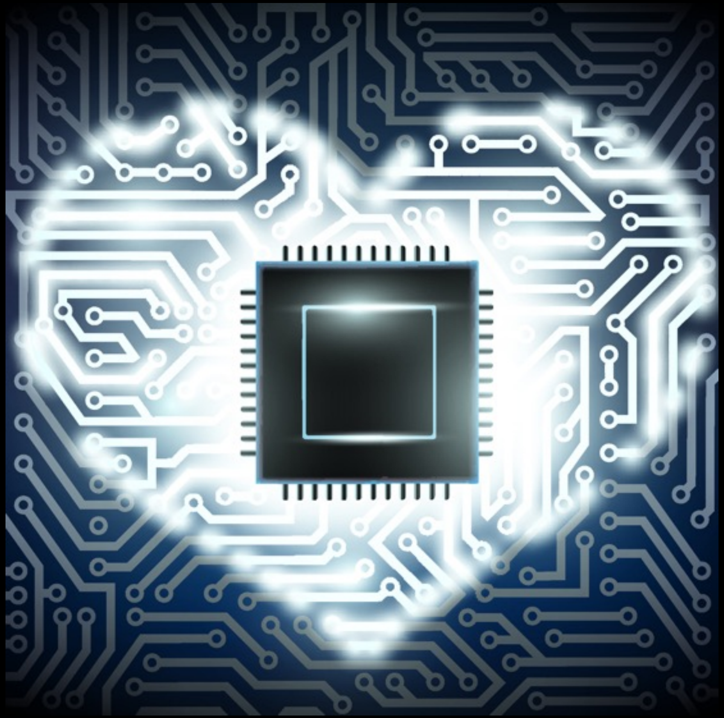
Debugging me

SINTEF

”We need to be able to verify the software that controls our lives”

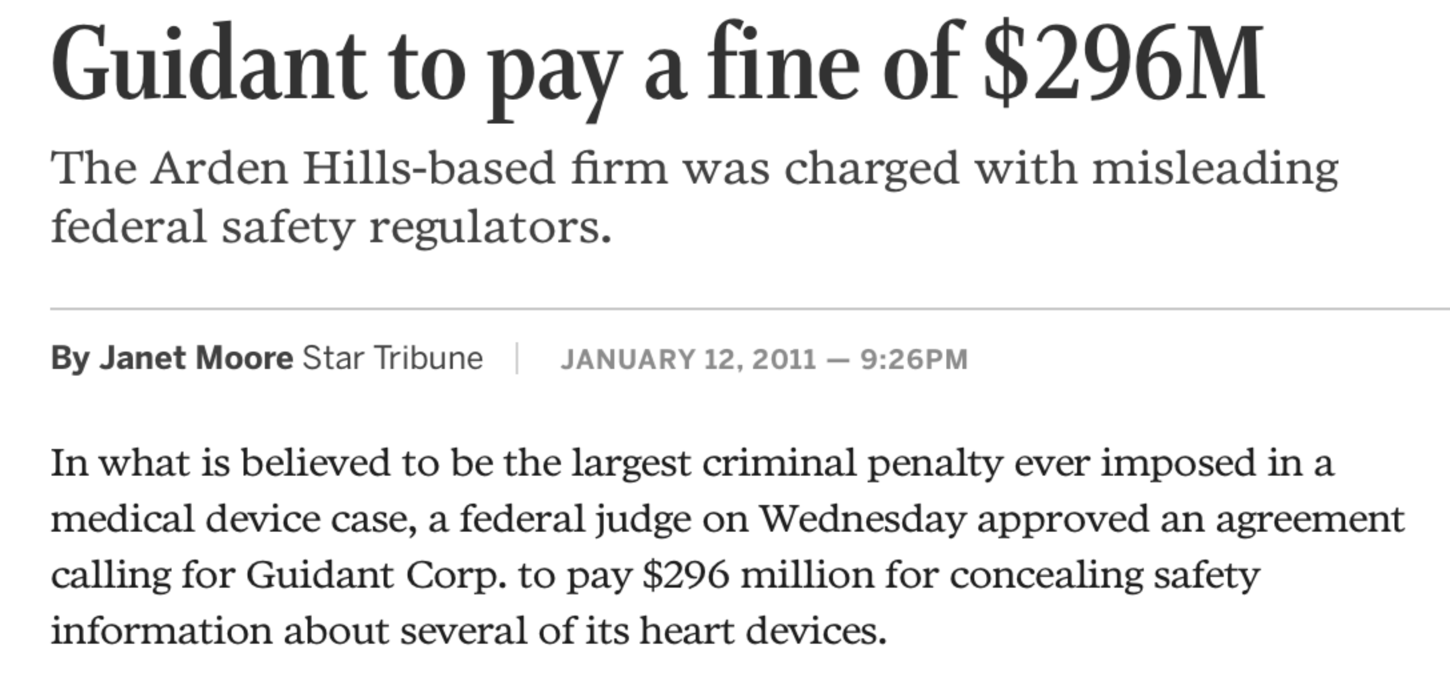
Bruce Schneier on “Volkswagen and Cheating Software”

Reflections on trusting machines



SINTEF

When trust is broken



Guidant to pay a fine of $296M

The Arden Hills-based firm was charged with misleading federal safety regulators.

By Janet Moore Star Tribune | JANUARY 12, 2011 — 9:26PM

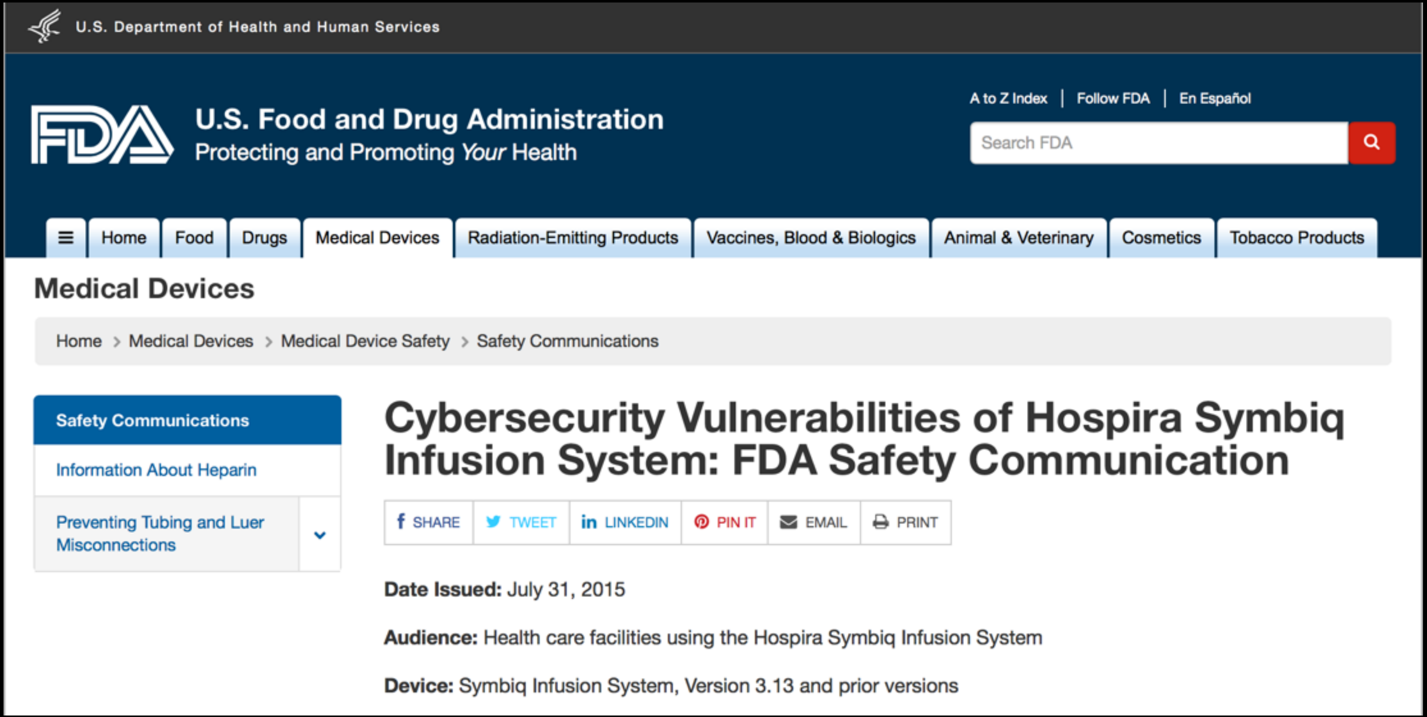
In what is believed to be the largest criminal penalty ever imposed in a medical device case, a federal judge on Wednesday approved an agreement calling for Guidant Corp. to pay $296 million for concealing safety information about several of its heart devices.

http://www.startribune.com/guidant-to-pay-a-fine-of-296m/113367264/

Previous work

- Kevin Fu et al:
  - Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses (2008)
  - Mitigating EMI signal injection attacks against analog sensors (2013)
- Barnaby Jack
- Hardcoded credentials
- Medical device honeypots
- Drug infusion pumps

Hacking can save lives!


U.S. Department of Health and Human Services
U.S. Food and Drug Administration
Protecting and Promoting *Your* Health
A to Z Index | Follow FDA | En Español
Search FDA
Home
Food
Drugs
Medical Devices
Radiation-Emitting Products
Vaccines, Blood & Biologics
Animal & Veterinary
Cosmetics
Tobacco Products
Home > Medical Devices > Medical Device Safety > Safety Communications
Safety Communications
Information About Heparin
Preventing Tubing and Luer Misconnections
SHARE
TWEET
LINKEDIN
PIN IT
EMAIL
PRINT

Medical Devices

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

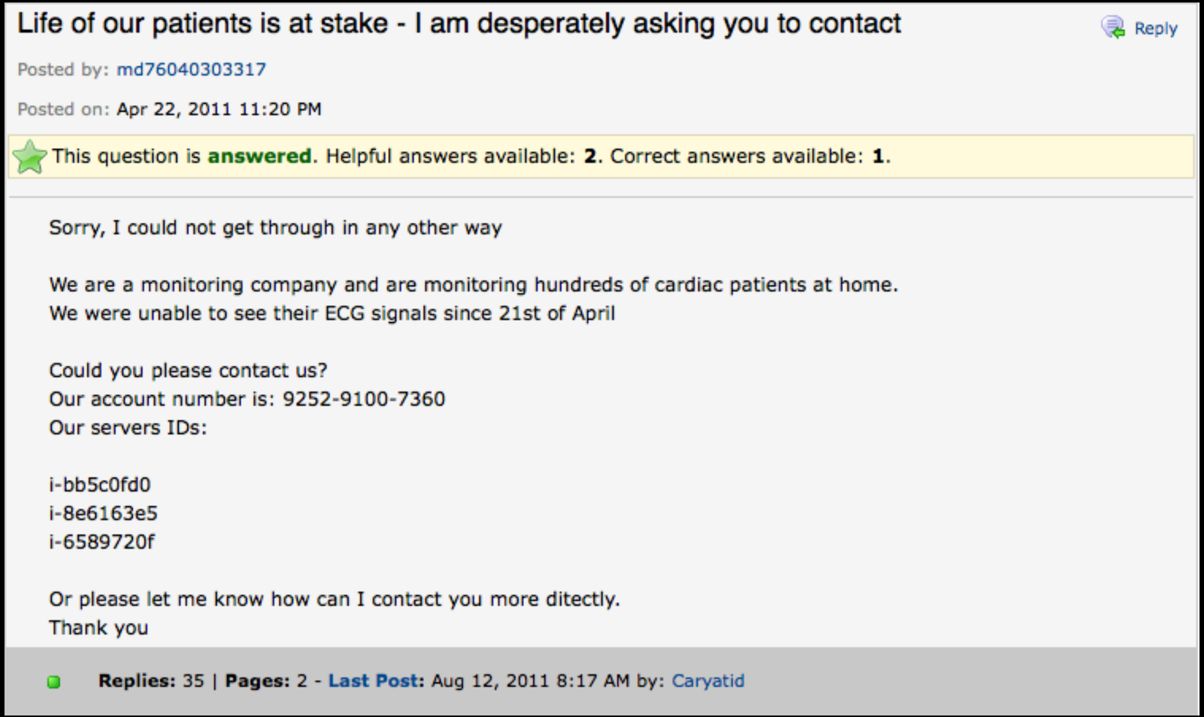
Date Issued: July 31, 2015

Audience: Health care facilities using the Hospira Symbiq Infusion System

Device: Symbiq Infusion System, Version 3.13 and prior versions

http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm

WTF are you doing with my data?



Life of our patients is at stake - I am desperately asking you to contact

Posted by: md76040303317

Posted on: Apr 22, 2011 11:20 PM

This question is **answered**. Helpful answers available: **2**. Correct answers available: **1**.

Sorry, I could not get through in any other way

We are a monitoring company and are monitoring hundreds of cardiac patients at home.
We were unable to see their ECG signals since 21st of April

Could you please contact us?
Our account number is: 9252-9100-7360
Our servers IDs:

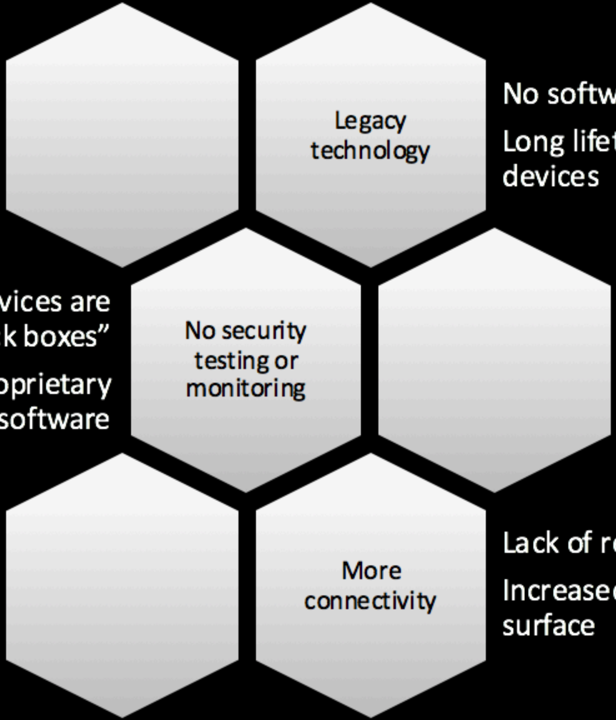
i-bb5c0fd0
i-8e6163e5
i-6589720f

Or please let me know how can I contact you more ditectly.
Thank you

Replies: 35 | **Pages:** 2 - **Last Post:** Aug 12, 2011 8:17 AM by: Caryatid

SINTEF

Why?



Legacy technology

No software updates

Long lifetime of devices

No security testing or monitoring

Medical devices are ”black boxes”

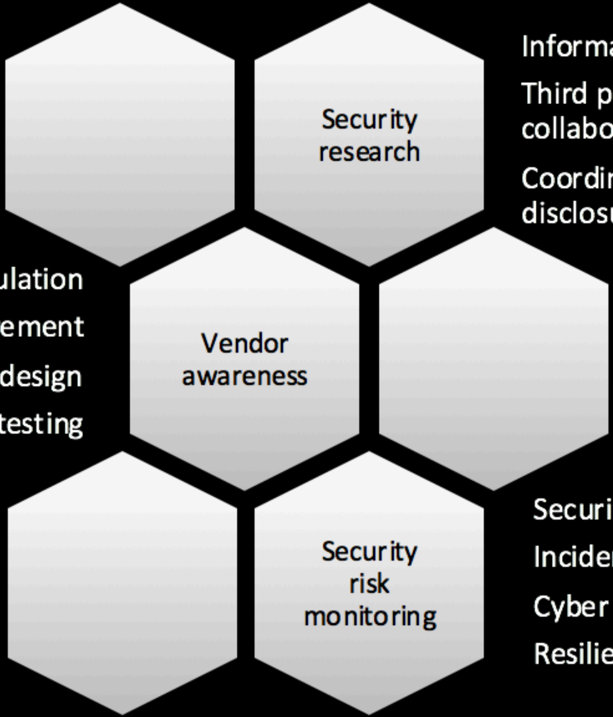
Proprietary software

More connectivity

Lack of regulations

Increased attack surface

How to solve it?



Security research

- Information sharing
- Third party collaboration
- Coordinated disclosure

Vendor awareness

- Regulation
- Procurement
- Safety by design
- Security testing

Security risk monitoring

- Security updates
- Incident response
- Cyber insurance
- Resilience

Hippocratic Oath

For Connected Medical Devices

Cyber Safety Capabilities What is your ready posture toward failure?

- **Cyber Safety by Design** – Anticipate and avoid failure
- **Third-Party Collaboration** – Engage willing allies to avoid failure
- **Evidence Capture** – Observe and learn from failure
- **Resilience and Containment** – Prevent cascading failure
- **Cyber Safety Updates** – Correct failure conditions once known

In Collaboration With

Security Researchers | Patients | Device Makers | Policy Makers | Insurers & Payers | Physicians & Care Givers | Standards Organizations | Healthcare Providers | Government Agencies

https://www.iamthecavalry.org/oath

Research needed

- Open source medical devices
- Medical device cryptography
- Personal area network monitoring
- Jamming protection
- Forensics evidence capture

SINTEF

The benefit outweighs the risk

I am The Cavalry

Credits

Éireann Leverett (@blackswanburst)

Tony Naggs (@xa329)

Gunnar Alendal (@gradoisageek)

Hugo Campos (@HugoOC)

Scott Erven (@scotterven)

Alexandre Dulaunoy (@adulau)

Claus Cramon Houmann (@ClausHoumann)

Joshua Corman (@joshcorman)

Beau Woods (@beauwoods)

Suzanne Schwartz (US FDA)

Family & Friends ❤

SINTEF

I am The Cavalry

Thank you!

marie.moe @ sintef.no

www.infosec.sintef.no
www.iamthecavalry.org

@MarieGMoe
@SINTEF_Infosec

SINTEF

TROOPERS