Oslo 18. april 2016

SINTEF

Teknologi for et bedre samfunn

Med hjertet på Internett

Sikkerhet i det medisinske IoT

Marie Moe, PhD, Forsker ved SINTEF IKT, Systemutvikling og sikkerhet

@MarieGMoe

@SINTEF_Infosec

NETT I HJERTET

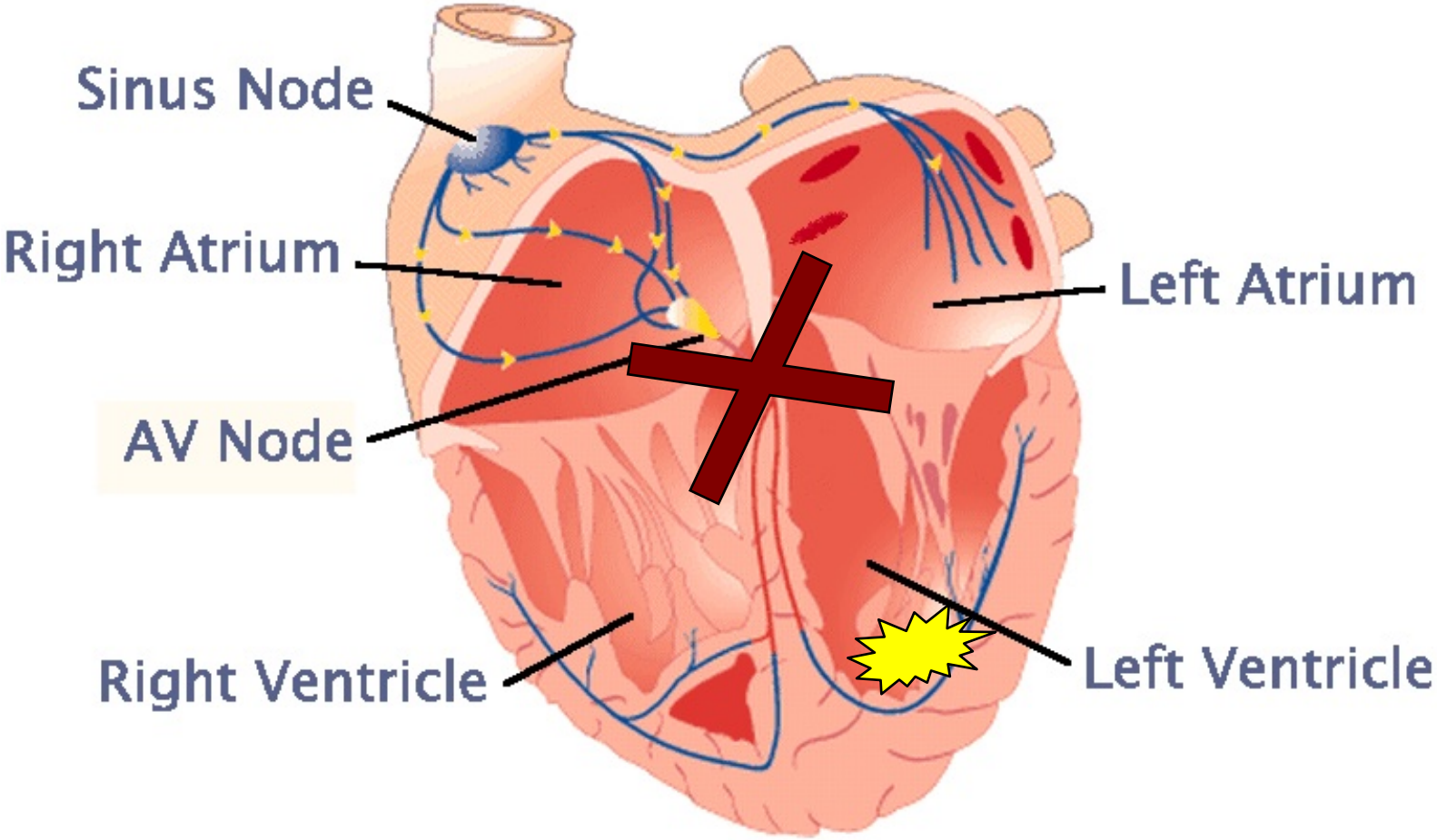
Da sikkerhetseksperten Marie Moe (37) fikk hjerteproblemer, oppdaget hun at det er mulig å hacke livskritiske, medisinske apparater som pacemakere, morfinpumper og insulinutstyr.

TEKST OSMAN KIBAR FOTO MAXIM SERGIENKO

Hamburg

Dagens Næringsliv Magasinet 9. januar 2016

Hjertets elektriske system

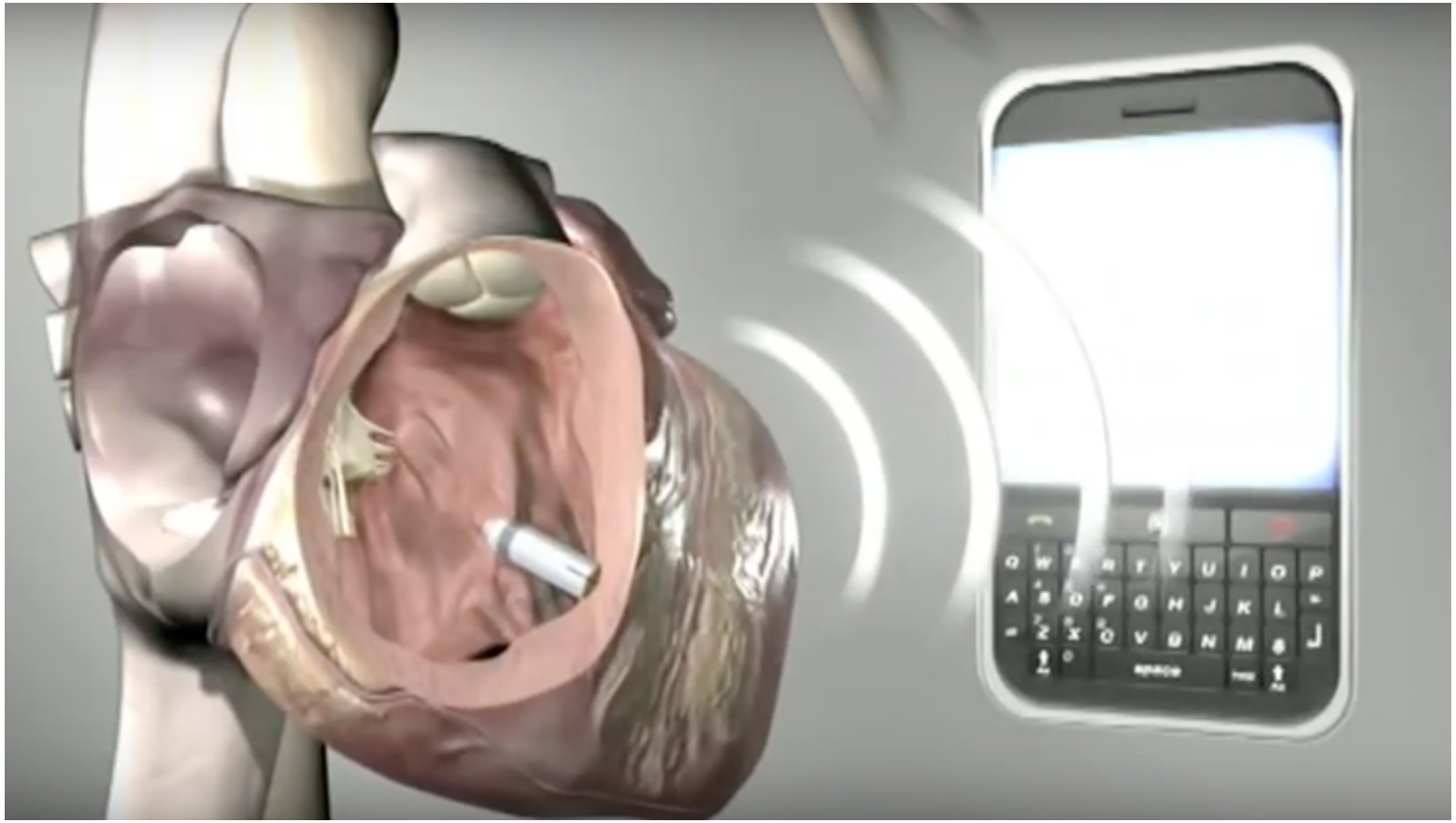


Pacemaker

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

Nyeste generasjon pacemaker

I en ganske nær fremtid...



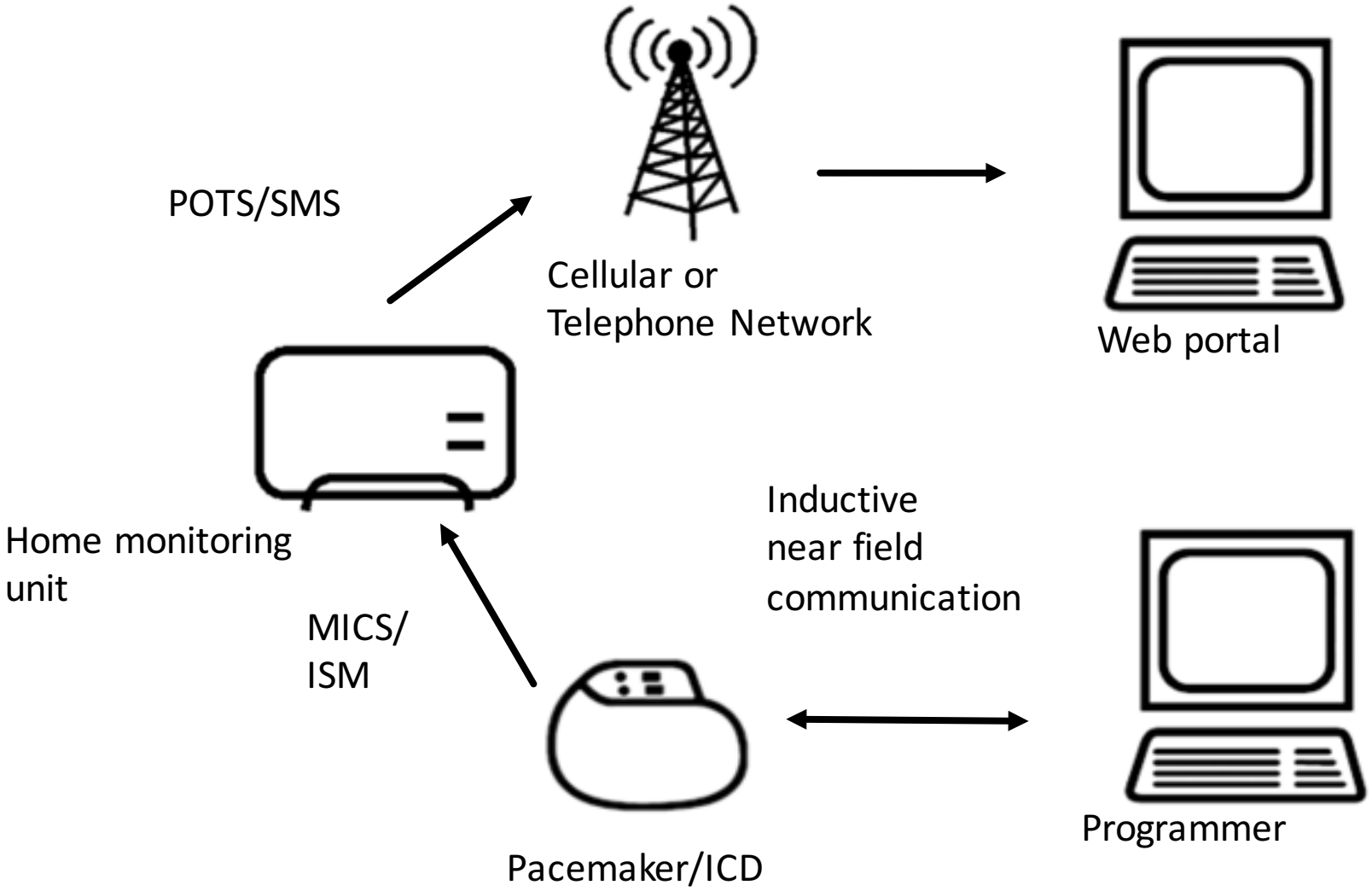
https://www.youtube.com/watch?v=ZiQJIpd2n8k

Fremtiden er nå

https://youtu.be/JzjXLtR5vkE?list=PLI6tVViVpg8gwKwWjYl8MOMUK8b0Rmm6v

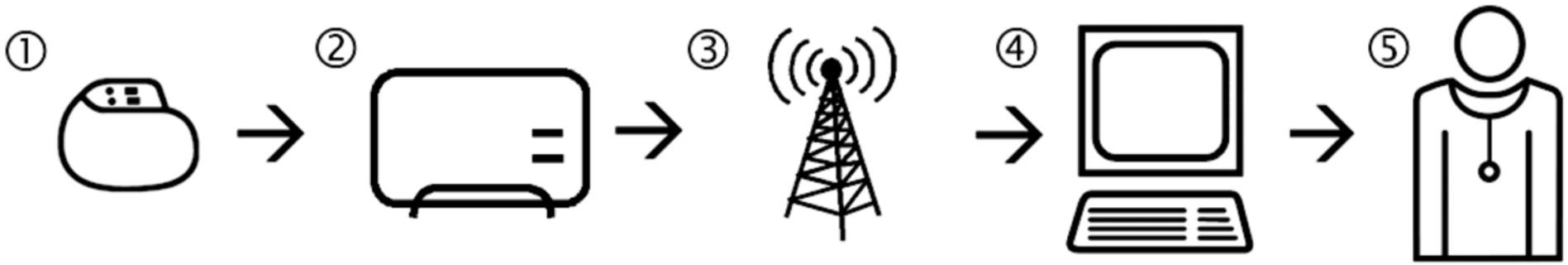
Det ”medisinske Internet of Things”

Når sensorsystemene implanteres i kroppen må vi beskytte vår personlige kritiske infrastruktur!


POTS/SMS
Cellular or
Telephone Network
Web portal
Home monitoring
unit
MICS/
ISM
Inductive
near field
communication
Programmer
Pacemaker/ICD

Hva kan gå galt?

- Sårbarheter i pacemakeren?
- Sårbarheter i aksesspunktet?
- Kan vi stole på mobilnettet?
- Er leverandørens server/skytjeneste sikret?
- Sårbarheter i web-portalen? Menneskelige feil?



Mulige konsekvenser

- Pasientinformasjon på avveie
- Tømming av batteri
- Feiltilstander og feilkonfigurasjon
- Livstruende feilbehandling
- Trusler og utpressing

Utfordringer for sikkerhet i medisinsk utstyr

- Proprietære løsninger uten velkjente og standardiserte protokoller
- Leverandør krever hull i brannmur for fjerntilgang
- Standard eller hardkodede passord, dårlig nøkkelhåndtering
- Ikke implementert tilfredsstillende mekanismer eller rutiner for software-oppdatering
- Det fysiske produktet har lang levetid og blir hengende etter i forhold til nye sikkerhetsmekanismer og utviklingen i trusselbildet
- Produkter som tradisjonelt har fungert i lukkede miljø kobles på nett
- Mangelfull regulering og lovverk
- Lav bruker- og bestillerkompetanse

Man kan ikke alltid stole på utstyrsleverandøren…

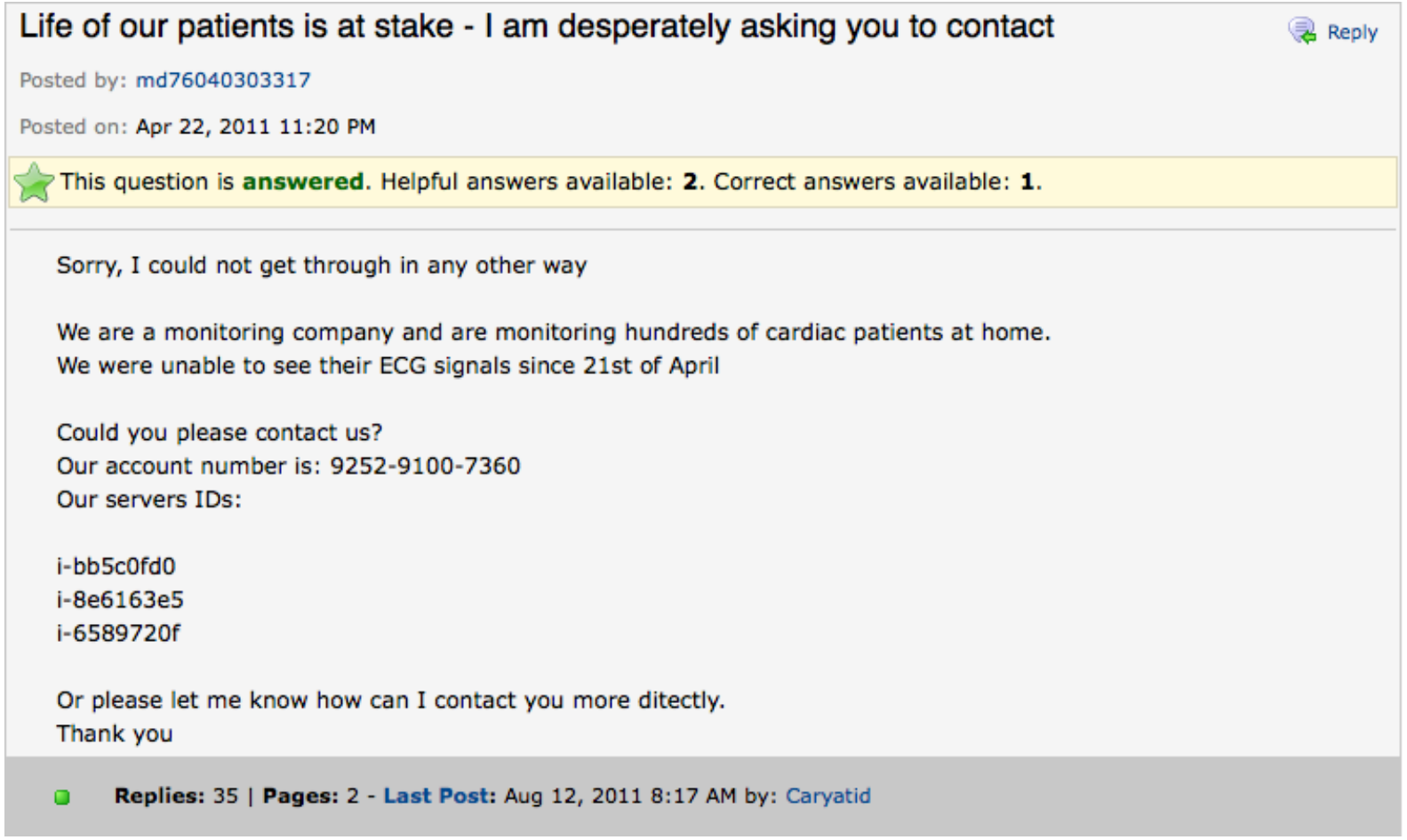
Guidant to pay a fine of $296M

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.

Hva skjer med min pasientdata i skyen?



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

Reply

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

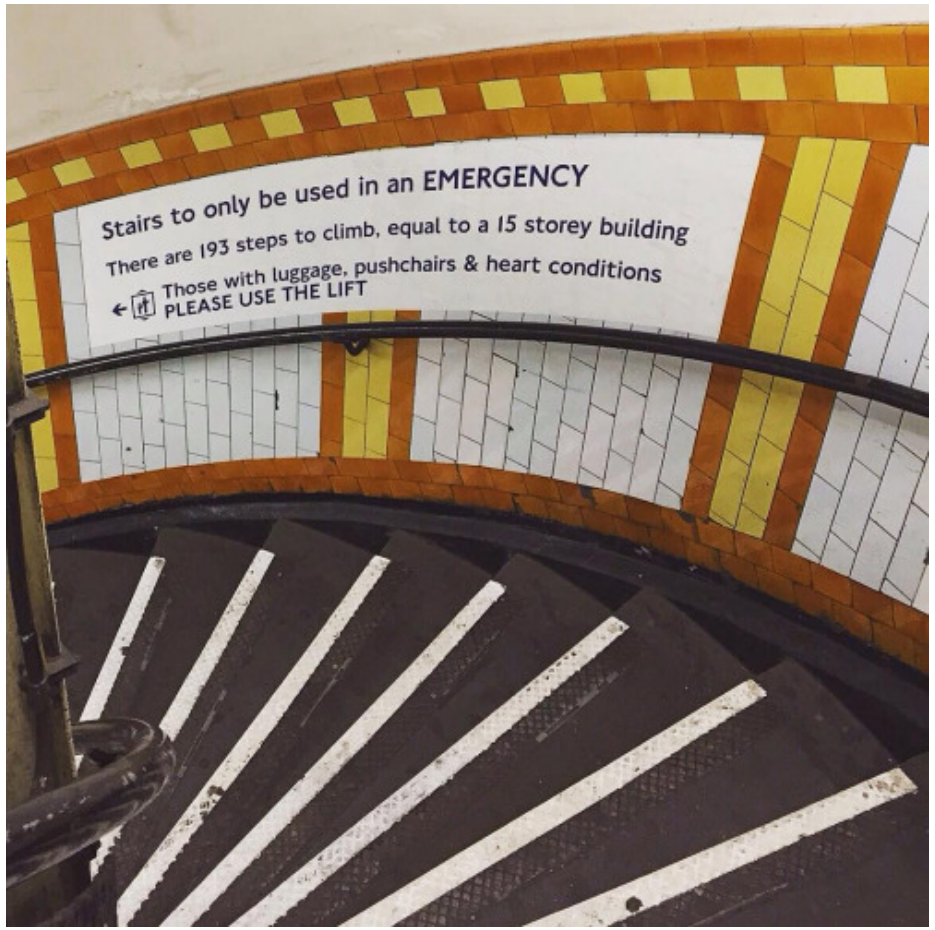
Could you please contact us?
Our account number is: 9252-9100-7360
Our servers IDs:

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

En veldig lang trapp...



Når det som står på skjermen ikke stemmer…

Fordelene utveier ulempene!

Jay Radcliffe: Hacket sin egen insulinpumpe

Hugo Campos: Tilgang til egen data fra ICD

Dr. Kevin Fu: Forsker på sikkerhet i pacemakere/ICDer

Noen referanser

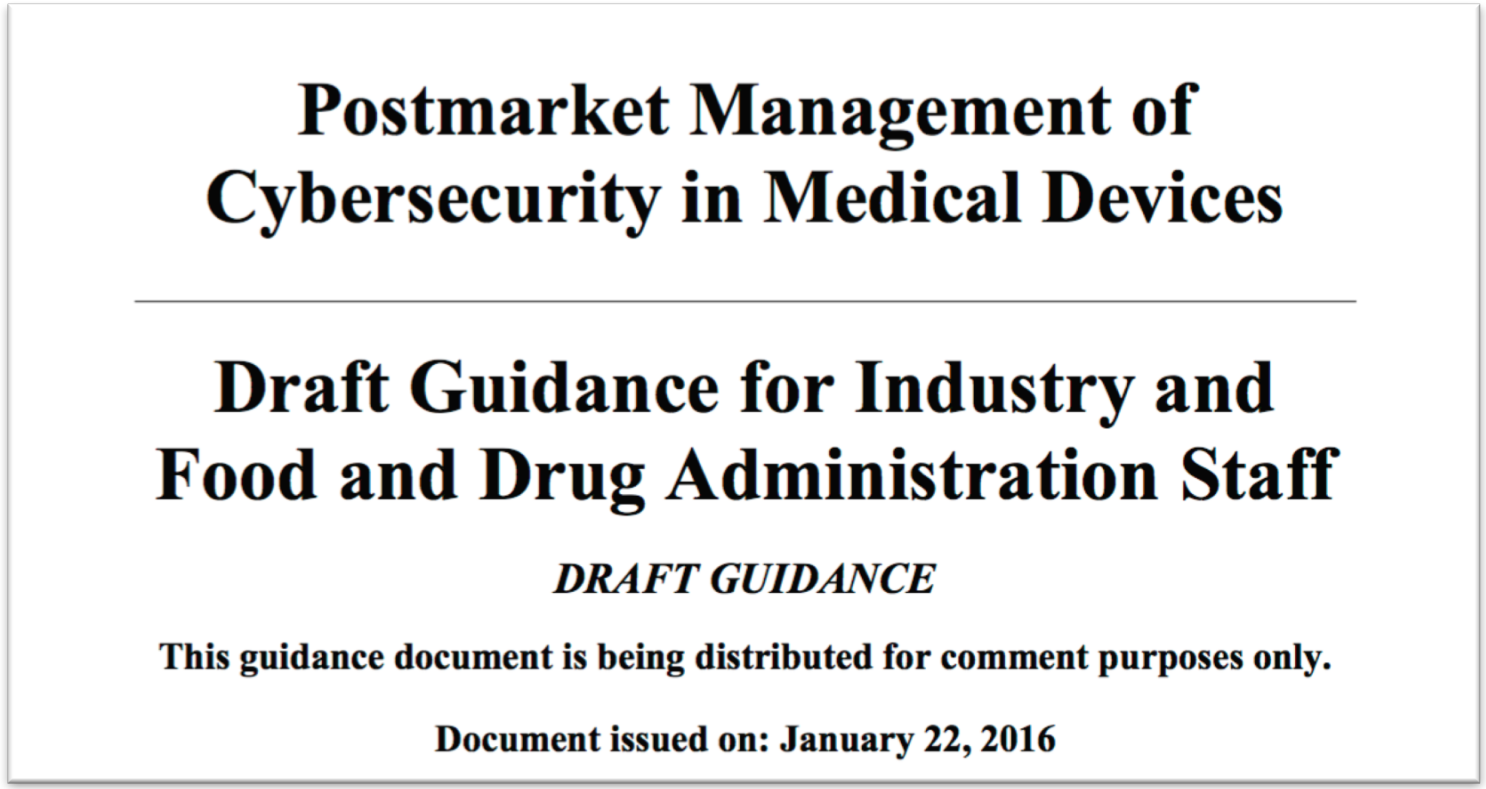
Pacemakere:

- 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

Annet medisinsk utstyr:

- Hardkodede passord og “medical device honeypots” (Scott Erven)
- Insulinpumper (Jay Radcliffe)
- Medisinpumper (Billy Rios)

Første eksempel på tilbaketrekking pga cybersikkerhet



Postmarket Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Document issued on: January 22, 2016

http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm

Hvordan få bedre sikkerhet?

- **Cybersafety-by-design**: Sikkerhet i programvareutviklingsløpet for medisinsk utstyr hos produsenter og i hele leverandørkjeden
- **Bevissikring:** Bevissikring og logging vil kunne brukes i hendelseshåndtering og etterforskning i etterkant av en hendelse der medisinske implantat kan ha blitt utsatt for cyberangrep
- **Testing**: Metodikk og rammeverk for tredjeparts testing
- **Patching:** Løsninger for rask og sikker patching av sårbarheter og sikkerhetshull i medisinske implantat
- **Resilience:** Hvordan sørge for at komponenter i det medisinske implantatet fortsetter å levere kritisk pasientbehandling også under feiltilstander eller forsøk på angrep

I Am The Cavalry

The Cavalry isn't coming... It falls to us

Problem Statement

Our society is adopting connected technology *faster than we are able to secure it*.

Mission Statement

To ensure connected technologies with the potential to impact public safety and human life are *worthy of our trust*.

Medical

Automotive

Connected Home

Public Infrastructure

Why Trust, public safety, human life
How Education, outreach, research
Who Infosec research community
Who Passionate volunteers
What Long-term vision for cyber safety

Collecting existing research, researchers, and resources
Connecting researchers with each other, industry, media, policy, and legal
Collaborating across a broad range of backgrounds, interests, and skillsets
Catalyzing positive action sooner than it would have happened on its own

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

https://www.iamthecavalry.org/oath

Konklusjon

Vår avhengighet av systemer som styres av programvare øker raskere enn vår evne til å sikre systemene

- Utstyrsprodusenter må bygge inn sikkerhet i produktene
- Brukere må gjøre egne risikoanalyser og følge med på utviklingen i risikobildet
- Vi må innse at det vil gå galt, og planlegge for dette
- Mer uavhengig forskning og tredjeparts testing trengs
- Standardisering, ansvarsavklaring og bedre lovregulering

Takk til

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)

Familie & venner ❤

SINTEF

Takk for oppmerksomheten!

marie.moe@sintef.no
http://infosec.sintef.no
http://iamthecavalry.org

@MarieGMoe
@SINTEF_Infosec