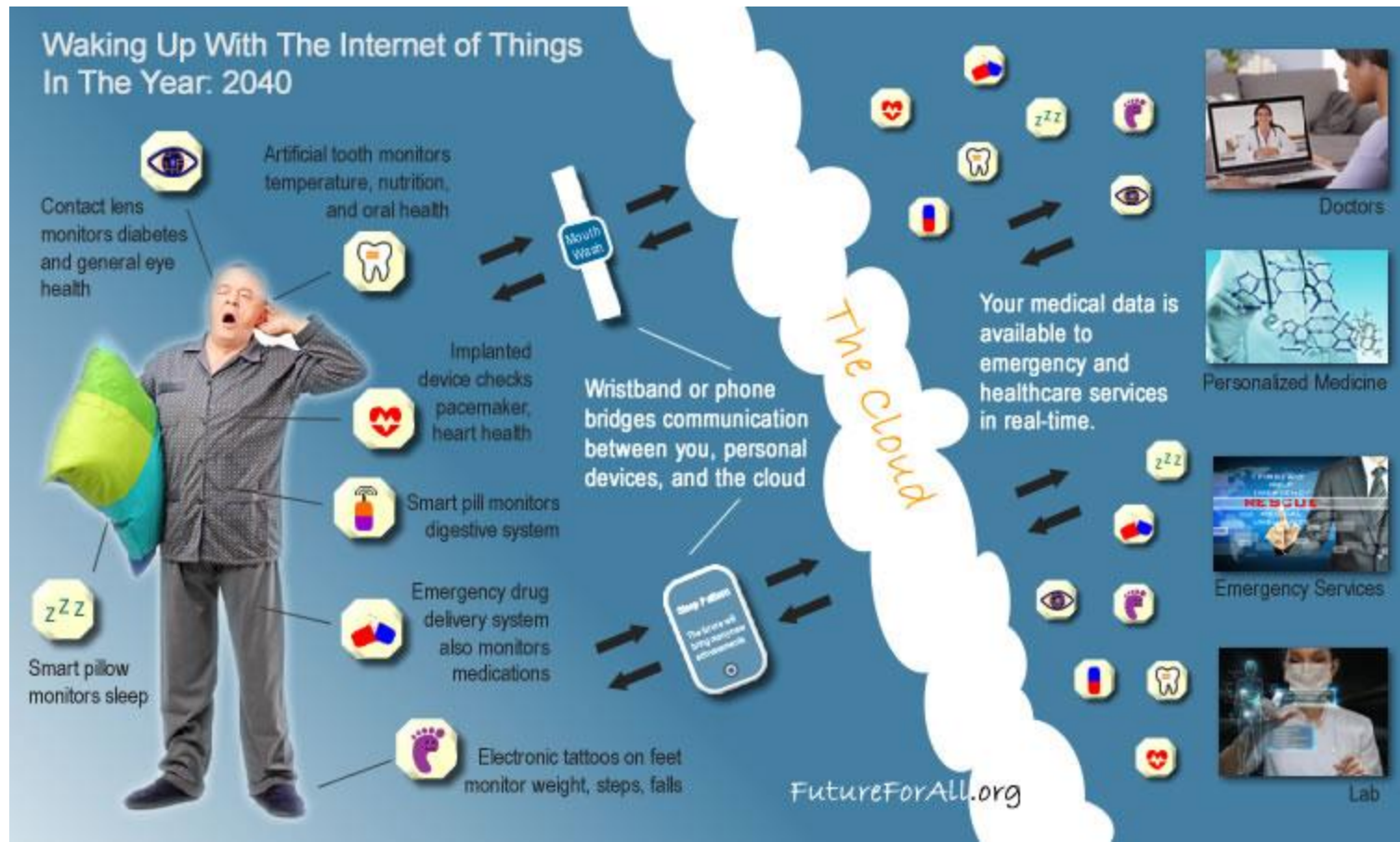


IoT in Healthcare and its security

Minatee Mishra,
Sr. Group Leader, Product Security, Philips HealthTech

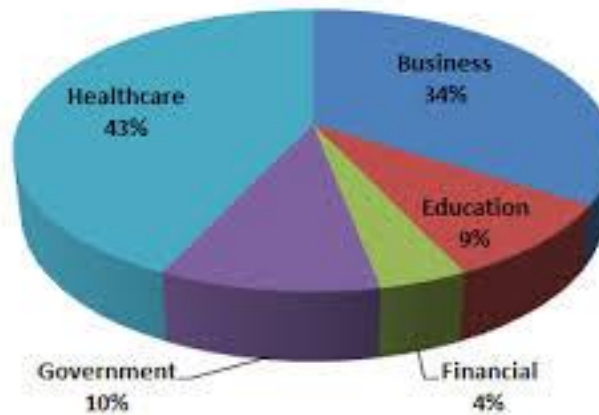
Jun 20, 2017

IoT in Healthcare



Threat Landscape

Data Breaches by Industry



Courtesy: nedocs.com

Dick Cheney Feared Assassination Via Medical Device Hacking: 'I Was Aware of the Danger'

By DAN KLOEFFLER and ALEXIS SHAW · Oct. 19, 2013

[Share with Facebook](#)

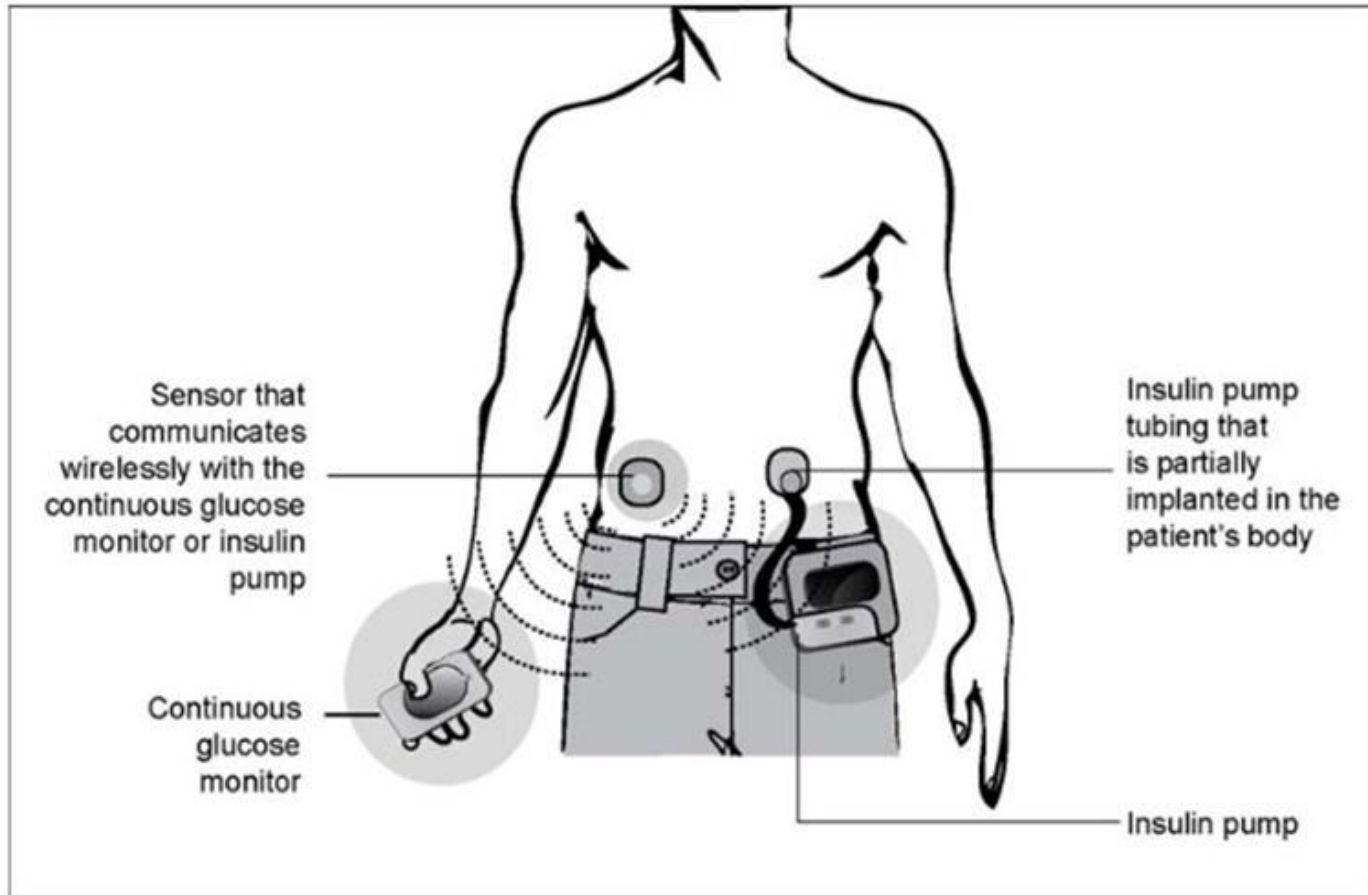
[Share with Twitter](#)



Courtesy: abdnews.go.com

PHILIPS

Insulin Pump Hacks



Source: GAO.

Courtesy: resources.infosecinstitute.com

PHILIPS

What was the issue?

- Sensitive Information leaked.
- Backdoor to device w/o authentication.
- Insecure firmware update.
- No authentication.



PHILIPS

What should device manufacturers do: Development

- 3 deadly sins

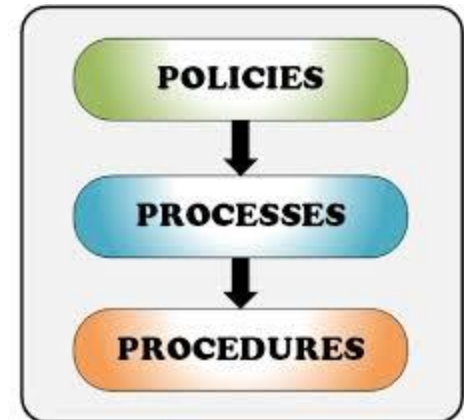


- 1 virtue

What should device manufactures do :

Process

- Security Governance
- Risk Management Framework
- Incident Management
- Vendor Management
- Secure Development
- Patch Upgrade process
- Training Process
- Responsible disclosure ..



What should device manufacturers do : Coordinated Disclosure



PHILIPS

Courtesy: Philips.com

Changing healthcare ecosystem

The screenshot displays the FDA Voice website interface. At the top, the U.S. Department of Health & Human Services logo is on the left, and the FDA U.S. Food & Drug Administration logo is in the center. The text 'FDA Voice' is prominently displayed on the right. Below the navigation bar, there are links for 'Blog Home', 'Categories', 'FDA.gov', and 'Contact Us'. The main content area features the NH-ISAC (National Health - ISAC) logo, which includes a globe and a heartbeat line. Below this, the ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) logo is visible, with the text 'Official website of the Department of Homeland Security' and 'INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM'. The main advisory is titled 'Advisory (ICSMA-17-009-01) St. Jude Merlin@home Transmitter Vulnerability', with an original release date of January 09, 2017. The advisory includes a 'Legal Notice' and an 'OVERVIEW' section. The 'OVERVIEW' section states that MedSec Holdings has identified a channel accessible by non-endpoint ('man-in-the-middle') vulnerability in St. Jude Medical's Merlin@home transmitter. It also mentions that the Food and Drug Administration (FDA) has released safety communication, Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter, to alert users about the identified vulnerability and corresponding mitigation as well as to provide recommendations to patients and healthcare providers. In response, NCCIC/ICS-CERT is releasing this advisory to provide additional information to patients and healthcare providers.

U.S. Department of Health & Human Services

FDA U.S. FOOD & DRUG ADMINISTRATION

FDA Voice

Blog Home Categories » FDA.gov Contact Us

← NH-ISAC NATIONAL HEALTH - ISAC

Official website of the Department of Homeland Security

ICS-CERT INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME ABOUT ICSJWG INFORMATION PRODUCTS TRAINING FAQ

Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

Advisory (ICSMA-17-009-01)
St. Jude Merlin@home Transmitter Vulnerability
Original release date: January 09, 2017

Print Tweet Send Share

Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

OVERVIEW

MedSec Holdings has identified a channel accessible by non-endpoint ("man-in-the-middle") vulnerability in St. Jude Medical's Merlin@home transmitter. St. Jude Medical has validated the vulnerability and produced a new software version that mitigates this vulnerability. A third-party security research firm has verified that the new software version mitigates the identified vulnerability.

This vulnerability could be exploited remotely. An attacker with high skill would be able to exploit this vulnerability.

The Food and Drug Administration (FDA) has released safety communication, Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter, to alert users about the identified vulnerability and corresponding mitigation as well as to provide recommendations to patients and healthcare providers. In response, NCCIC/ICS-CERT is releasing this advisory to provide additional information to patients and healthcare providers.

More Advisories

Courtesy: fda.gov, nhisac.org, ics-cert.us-cert.gov

PHILIPS

Thank You

Questions?



There are some viruses doctors can't treat.

- Security
- Fast response
- Control
- Minimized risk

PHILIPS