

Speak up for patient safety!

No one should be harmed
in health care



World Health
Organization



World
Patient Safety
Day 17 September



World Patient Safety Day – 17 September 2019

134 million adverse events occur each year due to unsafe care in hospitals in low- and middle-income countries, contributing to 2.6 million deaths annually!

Safety in health systems is a major global concern due to the enlarging numbers of people suffering avoidable harm while receiving healthcare.

Cyber-Security & IoT Teaser

Georg MACHER (TUG), Ceara TREACY (Lero)

18.09.2019

Overview

- Motivation & Brief Introduction to IoT
 - IoT Security Challenges
 - Security Basics
 - Teaser Afternoon Workshop
 - IoMT
 - Mobile Medical Apps (MMAs)
 - MMA Data in Flow
 - Cybersecurity Workshop
- Objectives



IoT Cyber-Security Market

- Identity & access management solution segment was valued at USD 255.8 million in 2017
- Market projection is USD 2.11 billion by 2025
- Smart home & consumer application segment dominated the market in 2017 and is projected to reach USD 2.93 billion by 2025
- IoT data security market will become the fastest growing segment in the IoT cybersecurity market, with revenues growing from \$3B in 2019 to \$7B in 2022

<https://www.grandviewresearch.com/press-release/global-internet-of-things-iot-security-market> , Sept 18
<https://ihsmarkit.com/research-analysis/cybersecurity-the-fastest-growing-iot-market.html> , June 19

News related to IoT Security



Hackers Remotely
Kill a Jeep on the
Highway—With Me
in It

Wired - 21.07.2015

News related to IoT Security



BBC

Sign in

News

Sport

Reel

Worklife

Travel

Future

NEWS

Home

Video

World

UK

Business

Tech

Science

Stories

Entertainment & Arts

Technology

Twitter CEO and co-founder Jack Dorsey has account hacked



Dave Lee

North America technology reporter

🕒 31 August 2019



Share

News related to IoT Security

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

FROM RUSSIA WITH LOVE —

VPNFilter malware infecting 500,000 devices is worse than we thought

Malware tied to Russia can attack connected computers and downgrade HTTPS.

DAN GOODIN - 6/6/2018, 3:00 PM

Twitter CEO and co-founder Jack Dorsey has account hacked



Dave Lee

North America technology reporter

🕒 31 August 2019



🔗 Share

News related to IoT Security

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

TechRepublic.

SEARCH



Developer Top DaaS providers Security More ▾

Amazon Echo randomly recorded and sent a Portland couple's conversation

A Portland couple claimed that their [Amazon Echo smart speaker recorded a conversation and transmitted it](#) to someone in their contact list—an employee of the couple—in Seattle. The original report is suspect, though [Amazon confirmed to CNET that the incident occurred as described](#).

The model of the Echo Dot photographed in the original report is capable of outputting sound to an external speaker through a 3.5mm audio cable. If a speaker was attached to the Echo Dot, but turned off, the microphone in the Echo Dot unit would still be active, though it would have been impossible for the owners to hear an audio prompt through the speaker. The original report fails to mention this possibility, likewise, the report fails to correctly identify the device as an Amazon Echo.



🕒 31 August 2019



News related to IoT Security

CyberDB
The Cyber Research Databank

ABOUT

DATABASE

PURCHASE

CARS GAMING & CULTURE

5 providers Security More ▾

couple's

ded a conversation and
e-in Seattle. The original
occurred as described.

of outputting sound to an
ed to the Echo Dot, but
ugh it would have been
. The original report fails
re device as an Amazon

Top 10 Sectors Breached

(Ordered by Number of Identities Exposed)

Rank	Sector	Number of Identities Exposed	Percentage of Identities Exposed
1	Retail	205,446,276	59%
2	Financial	79,465,597	23%
3	Computer Software	35,068,405	10%
4	Healthcare	7,230,517	2%
5	Gov. and Public Sector	7,127,263	2%
6	Social Networking	4,600,000	1%
7	Telecom	2,124,021	.6%
8	Hospitality	1,818,600	.5%
9	Education	1,359,190	.4%
10	Arts and Media	1,082,690	.3%

Source: Symantec



B B

NE

Home

Techr

Tw
has



🕒 31 August 2019

T     share



Search|

BB

NE

Techr

Two
has



Medical Security Nightmares

Things Hackers don't want to see as a patient in a hospital

 Florian Grunow

Privacy?

Source: Symantec

```
POST /cgi-bin/maint HTTP/1.1
User-Agent: vendor UserAgent
Host: scalew.vendor.net
Accept: /*/*
Content-Length: 12901
Content-Type: application/x-www-form-urlencoded
Expect: 100-continue
```

[illegible]

re device as an Amazon



T



Share

News related to IoT Security

**BUSINESS
NEWS DAILY**
Small Business Solutions & Inspiration

START
Your Business

GROW
Your Business

BUILD
Your Career

LEAD
Your Team

FIND
A Solution



SALES & MARKETING

FINANCES

YOUR TEAM

TECHNOLOGY

SOCIAL MEDIA

SECURITY

B

Product and service reviews are conducted independently by our editorial team, but we sometimes make money when you click on link

N

Home

[Grow Your Business](#) » [Technology](#)

The Security of Connected Medical Devices

Tec

By Adam C. Uzialko, Writer | [May 10, 2019](#) 07:00 am EST

0 0 0

**Tv
ha**



31

- The **healthcare industry is very vulnerable to cyberattack.**
- The most **common types of threats are ransomware, malware, data breaches, DDoS** and cryptojacking.
- Patient care and safety, data loss, and damage to a healthcare provider's reputation are among the consequences of networks being attacked.
- To stop cyberattacks on medical devices, you need to monitor and segment devices, keep software updated, and implement a response plan to an attack.

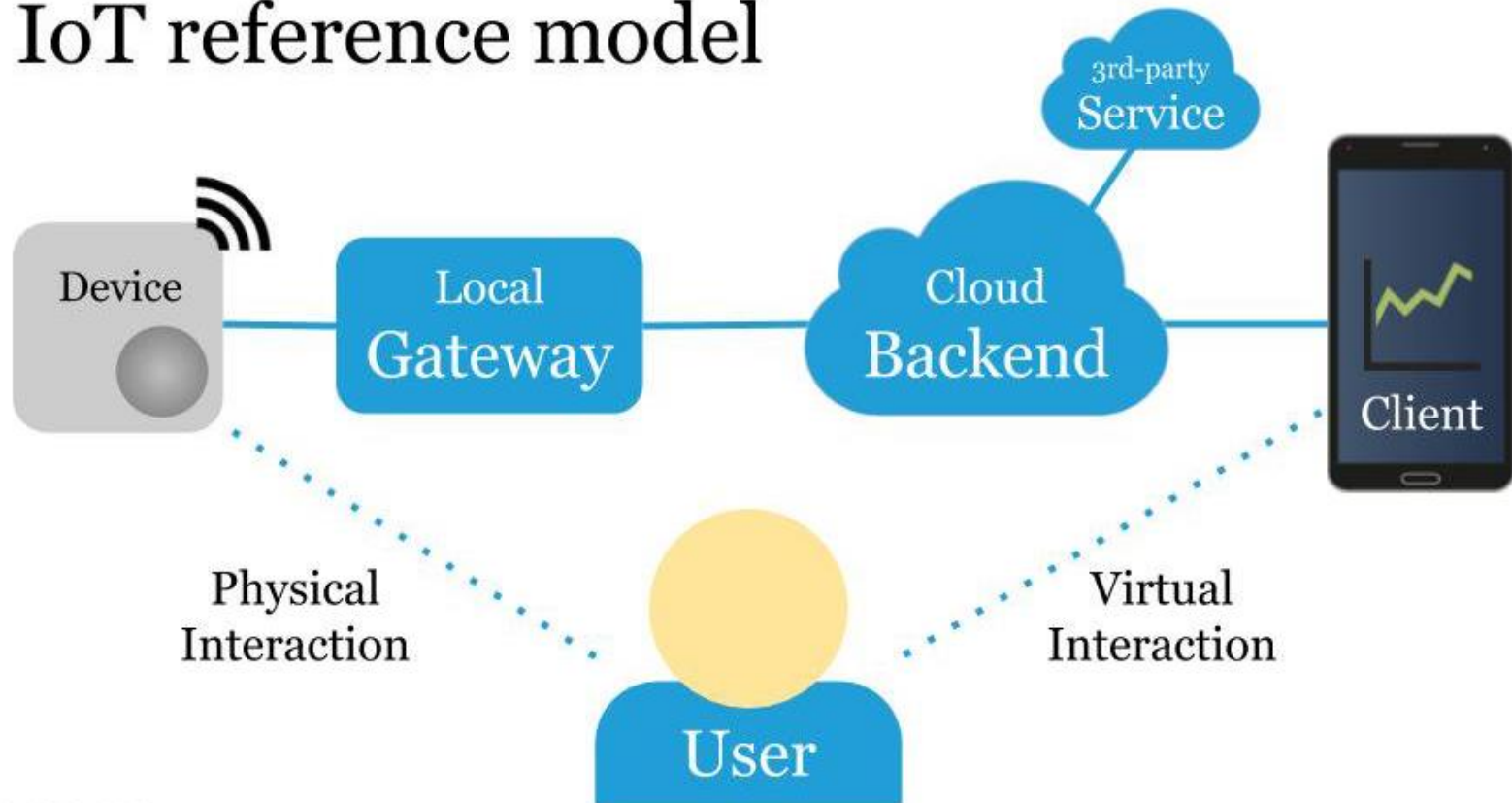


Typical IoT Architectures



Typical IoT Architectures

IoT reference model



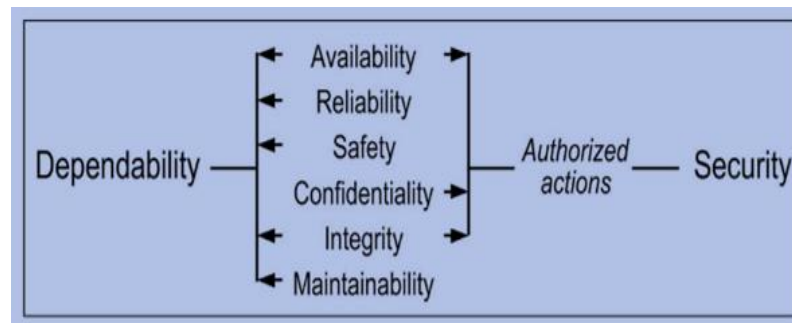
Differences between IT and IoT (excerpt)

	IT	IoT
Device volumes	Limited number per institution	Very large volume
Device types	quasi standardized	Wide variety of custom devices
HW / SW	quasi standardized	Custom
Management & Control	quasi standardized	Mostly unmanaged
Devices access	Restricted	Quasi public
Risk	Data, revenue & reputation losses	+ life threatening impacts
Connectivity	Private networks & central connection to WWW	ubiquitous

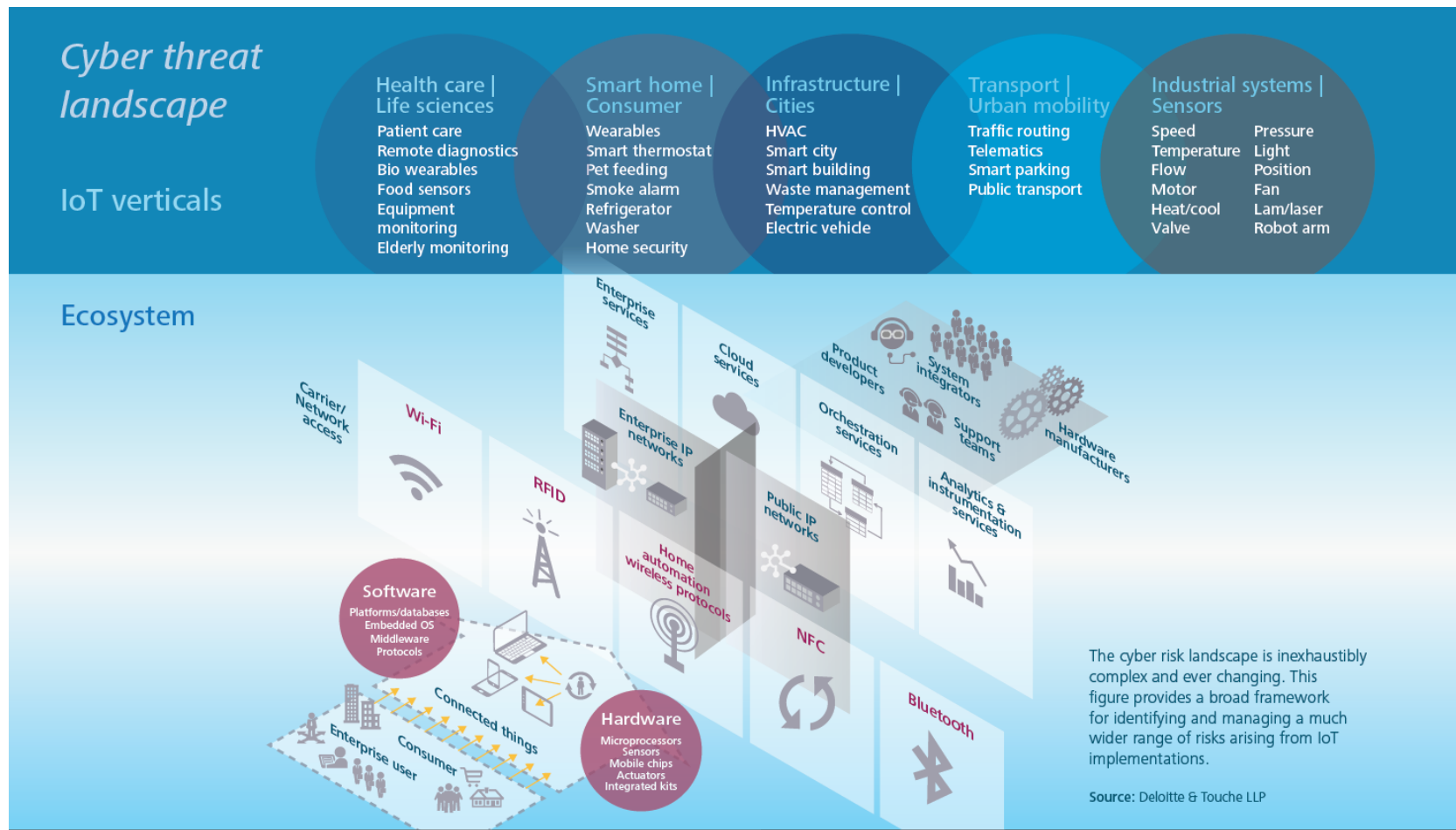
IoT and balancing of the forces



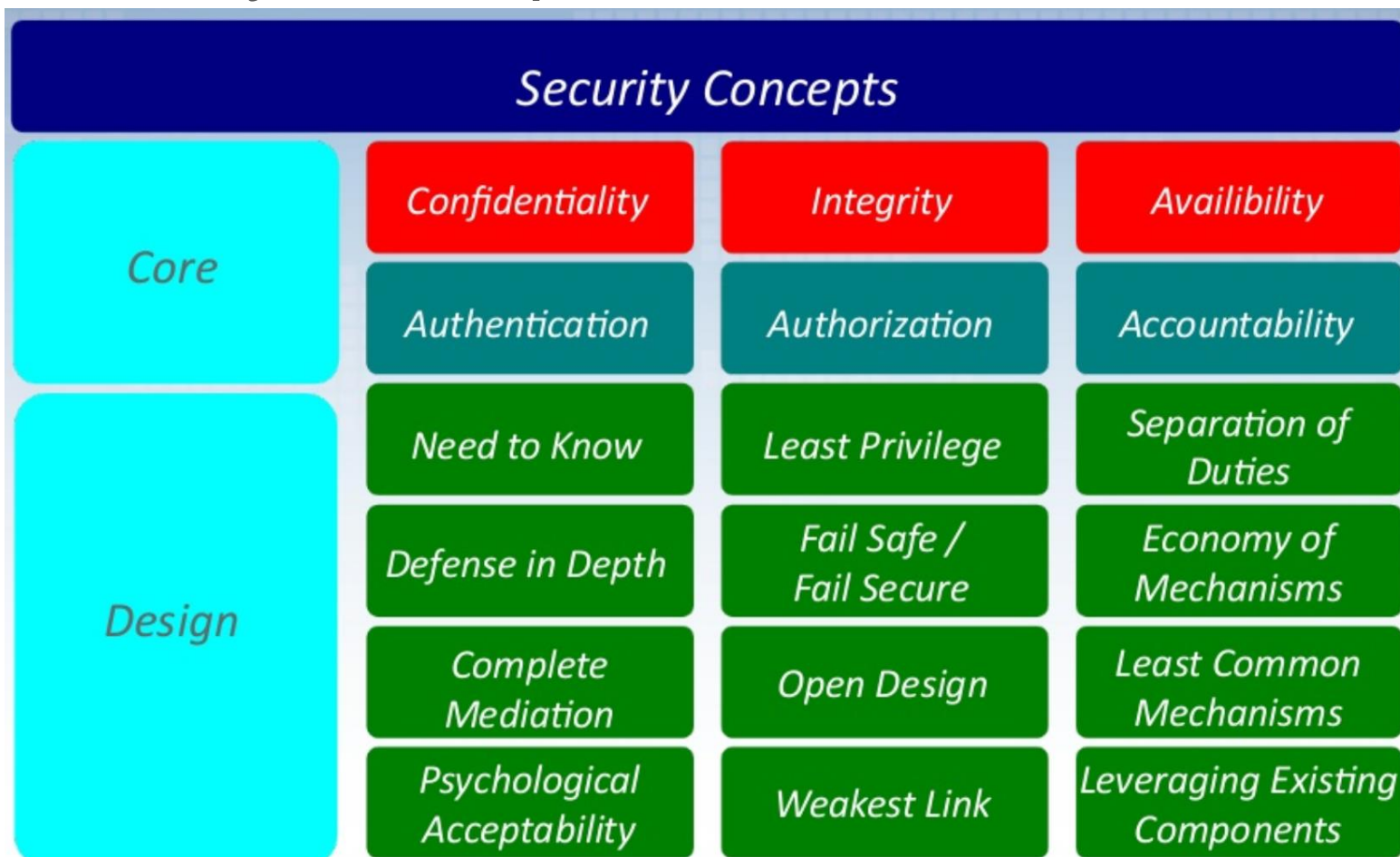
- **availability** (Sec.): readiness for correct service
- reliability: continuity of correct service
- safety: absence of catastrophic consequences on the user(s) and the environment
- **integrity** (Sec. - “improper” meaning “unauthorized.”): absence of improper system alterations
- maintainability: ability to undergo modifications and repairs
- **confidentiality** (Sec.): the absence of unauthorized disclosure of information



Internet of Things and the Cyber Threat Landscape



Security Concepts



GDPR Requirement - 'Privacy by Design'

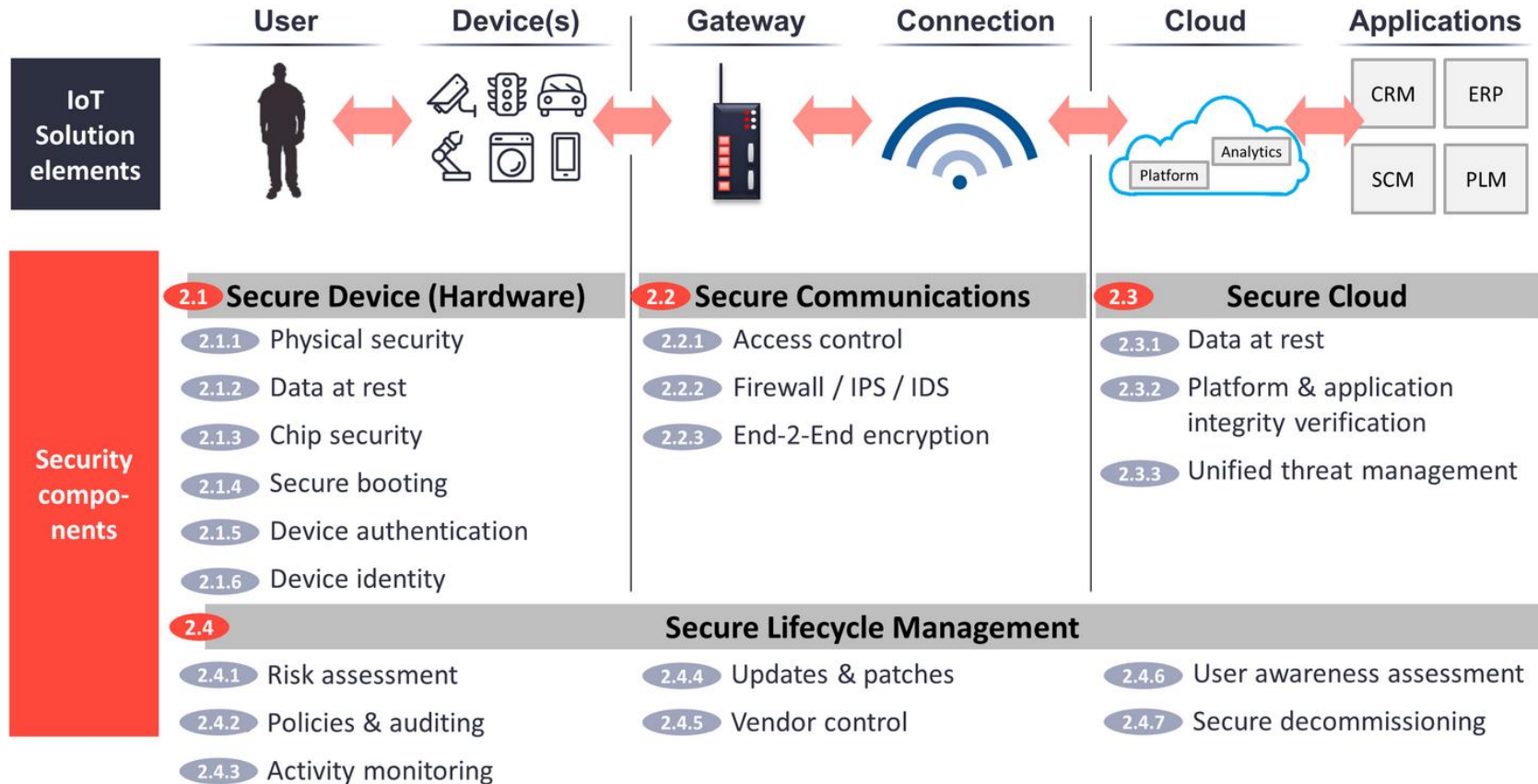
Cyber-Security at Development Time

- Security Development Lifecycle (SDL) required
 - Understand threat vectors
 - Understand risks and exposure possibilities
 - Set risk management
 - Identify security solutions & architecture approaches

Cyber-Security at Development Time

- Security Development Lifecycle (SDL) required
 - Understand threat vectors
 - Understand risks and exposure possibilities
 - Set risk management
 - Identify security solutions & architecture approaches
- Security must be incorporated holistically
 - Device design
 - Manufacturing
 - Testing and validation
 - Post-purchase maintenance and aftermarket

Security happen on multiple layers



Source: IoT Analytics

© <https://iiot-world.com/reports/an-overview-of-the-iot-security-market-report-2017-2022/>

Internet of Medical Things - IoMT

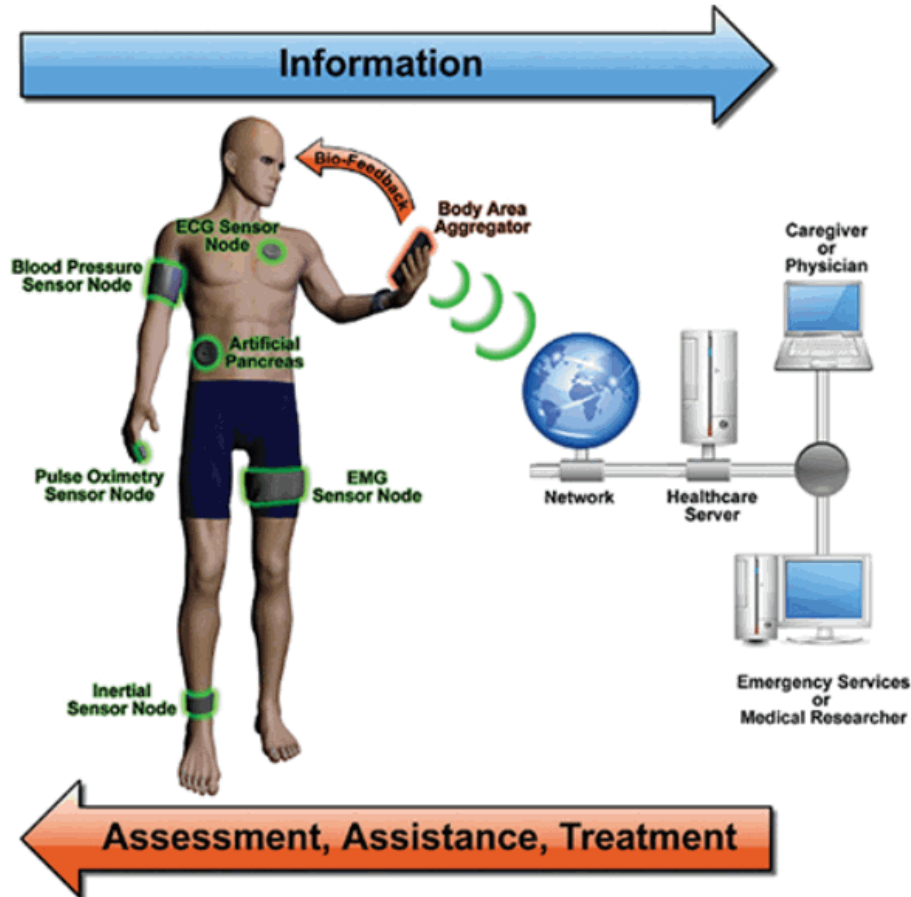


- IoMT – a connected infrastructure of health systems and services.

<http://medgizmo.info/news/internet-of-things-iot-healthcare-applications/>

<https://investimpactly.org/2017/06/29/how-iomt-can-help-meet-elderly-health-care/>

Internet of Medical Things - IoMT



Sensors connected on a patient for Remote Health Monitoring

<http://medgizmo.info/news/internet-of-things-iot-healthcare-applications/>

<https://investimpactly.org/2017/06/29/how-iomt-can-help-meet-elderly-health-care/>



- IoMT – a connected infrastructure of health systems and services.
- Mobile Medical Apps (MMAs) are a part of IoMT

THE INTERNET OF (MEDICAL) THINGS TECHNOLOGY

3.7M Medical devices in use today connecting to & monitoring various parts of the body

Active implantable medical devices control stimulation &/or precision medicine therapy to treat disease & improve patient quality of life.



Monitors medical conditions specific to patient's disease & other systemic conditions such as heart rate, blood sugar, exercise, etc.

Closed-Loop System
"Smart" software supports device iteration based on data inputs to deliver best patient therapy

One IOMT system solution collecting data from medical devices, medications, & biometrics to modify therapeutic window towards best care option



97% Wi-Fi adoption rates in hospitals
10% Medical devices enabled with Wi-Fi

OPTIMIZED RESULTS FOR:

PATIENTS...



Receive **individually-optimized care** faster, with few doctor office visits, and decreased overall time "thinking" about the disease

HEALTHCARE PROFESSIONALS...



Monitor patient status, disease progression, & device performance. This allows for:

- Enhanced patient support
- Reduced risk
- Feedback on device design improve opportunities

PATIENT FAMILIES...



Can be included in regular communications to **help monitor or reassure assurance** of patient wellness.

HEALTHCARE SYSTEM...



Automated monitoring & verification of advanced products to **eliminate human error & falsification**

NEXEON

IoMT and Cybersecurity

- The scale and cost of breaches is often significant and far reaching. Need to safeguard patient safety, maintain the security and privacy of patient information. Breaches of health information can have serious consequences for:
 - Patients harm or wellbeing
 - An organisation, including reputational and financial harm. (Deloitte 2019)

IoMT and Cybersecurity

- The scale and cost of breaches is often significant and far reaching. Need to safeguard patient safety, maintain the security and privacy of patient information. Breaches of health information can have serious consequences for:
 - Patients harm or wellbeing
 - An organisation, including reputational and financial harm. (Deloitte 2019)
- MMAs are being developed persistently without proper security application, principally due to the lack of:
 - Regulation requirements - General Data Protection Regulation (GDPR), raises compliance issues in the domain of consent, could help towards more secure IoMT use cases.
 - Understanding of current standards - is a lack of specific standards tailored to IoMTs security
 - Best practice pertaining to data security in healthcare – lack of training and experience

Issues Security of MMA and IoMT

- There is a lack of specific standards tailored to IoMTs security

Issues Security of MMA and IoMT

- There is a lack of specific standards tailored to IoMTs security
- The increased flow of information from IoMTs endpoints and applications increases the risk landscape; therefore, their security needs to be addressed.

Issues Security of MMA and IoMT

- There is a lack of specific standards tailored to IoMTs security
- The increased flow of information from IoMTs endpoints and applications increases the risk landscape; therefore, their security needs to be addressed.
- The moment you deploy applications, they're vulnerable, creating the broadest attack surface for patient data and an organisation

Issues Security of MMA and IoMT

- There is a lack of specific standards tailored to IoMTs security
- The increased flow of information from IoMTs endpoints and applications increases the risk landscape; therefore, their security needs to be addressed.
- The moment you deploy applications, they're vulnerable, creating the broadest attack surface for patient data and an organisation
- Most precarious state is MMA data flowing across open networks and unknown systems due to it's exposure to more threats which increases the vulnerability.

What is a MMA - US FDA Categorisation

Medical Mobile Apps Focus of FDA Regulatory Oversight

Mobile apps that connect to a medical device for the purpose of controlling the operation of the device - e.g., an app that alters infusion pump settings.



Apps that:

- display, transfer, convert or store patient-specific data from a connected device
- transform a mobile platform into a medical device

Mobile Apps for which FDA Intends to Exercise Enforcement Discretion

Mobile apps that help asthmatics track inhaler usage, asthma episodes experienced, location of user at the time of an attack, or environmental triggers of asthma attacks.



Mobile Apps that are NOT Medical Devices

FDA released draft guidance General Wellness: Policy for Low Risk Devices Draft Guidance for Industry and FDA Staff, January 20 2015.

Mobile apps that are intended for general patient education and facilitate patient access to commonly used reference information.



What is a MMA –Europe Categorisation

- July 2016, the European Commission issued a guidance “*Qualification and Classification of Standalone Software*” to assist the app developers in qualifying their software as a medical device. In EU, health-related apps, generally known as mHealth apps, are categorized as:
 - Medical Apps: Generally used in prevention, diagnosis, and treatment of diseases (CE certification is required for these apps).
 - Non-Medical Apps: Related to fitness, lifestyle, and well-being.
- Several EU member states such as France, Spain, Germany, and Italy are participating in developing the guidance for MMAs to provide clarification on the European Commission guidelines.

What is Data in Flow

- The term data flow was published in ISO/IEC 2382-7:2000 Information technology – Vocabulary - Part 7: Computer programming (ISO/IEC 2000) remains unchanged in the revised 2015 standard. Data flow is:

“...movement of data through the active parts of a data processing system in the course of the performance of specific work”

[(ISO/IEC 2382:2015, 2121825(ISO/IEC 2015a)]

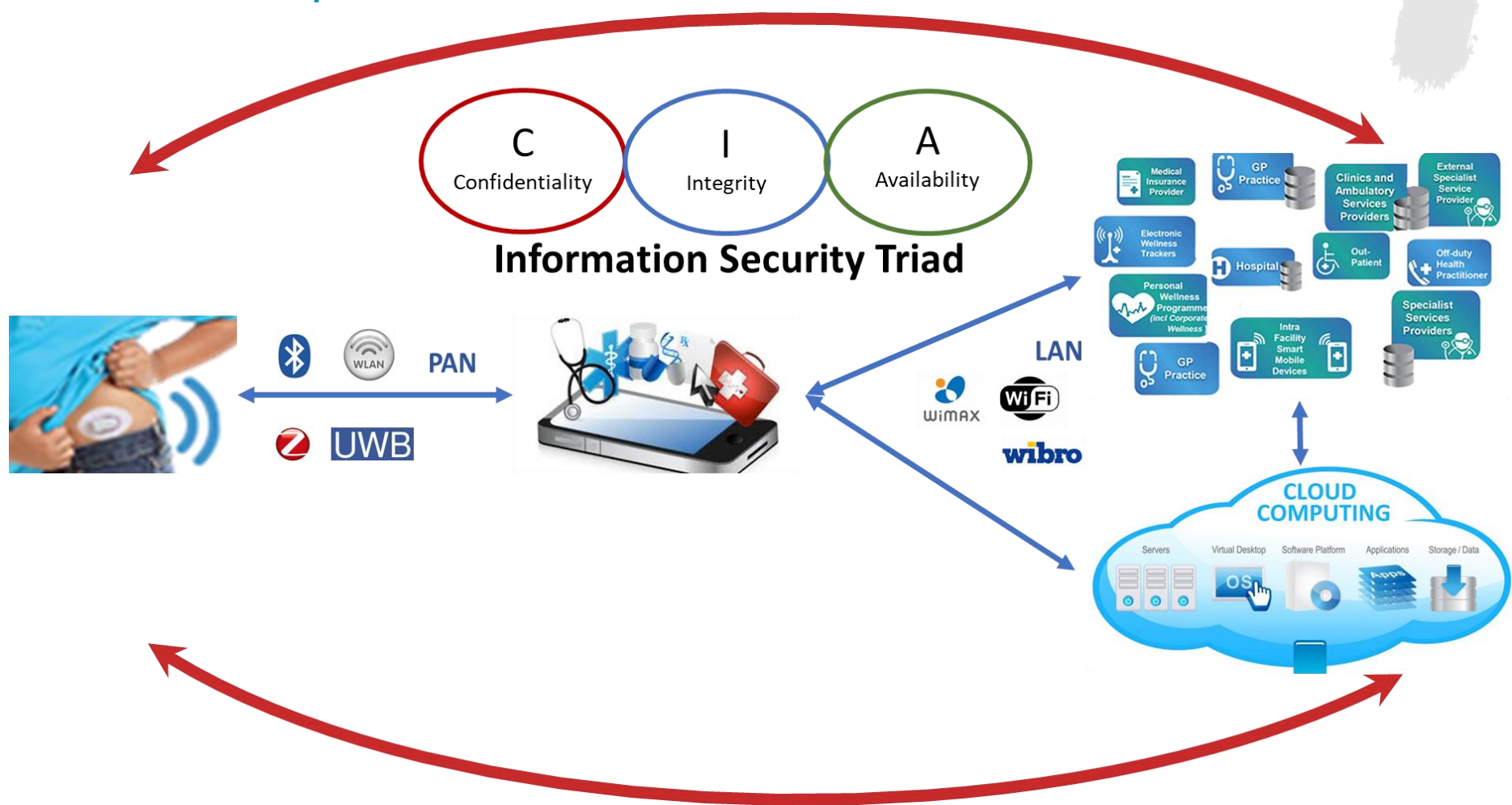
- Context of my research, data flow is the path data and information takes through a system comprised of software, hardware or a combination of both, that includes all nodes through which the data travels, from its original source to its end users.



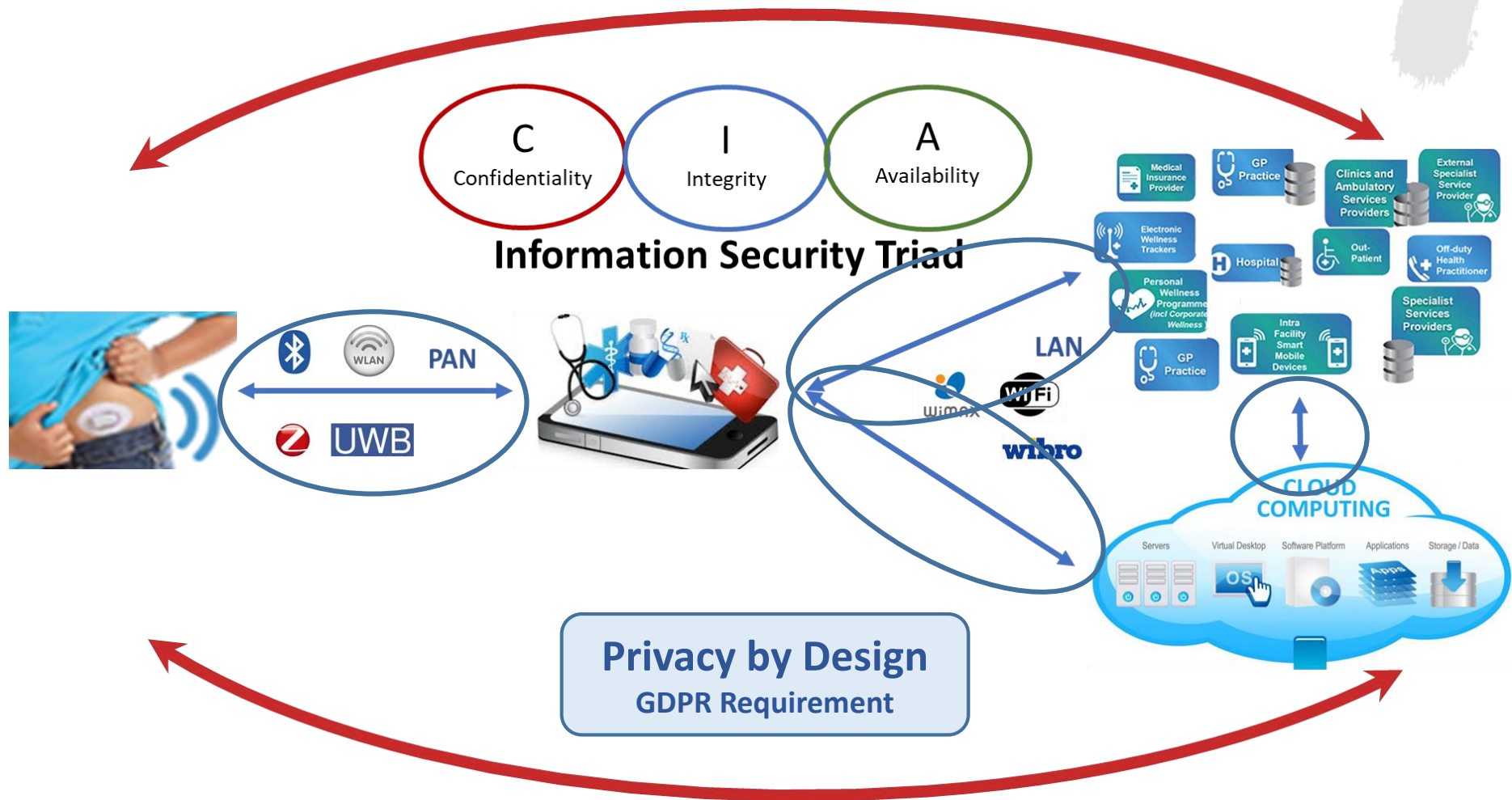
DKIT

REGULATED SOFTWARE
RESEARCH CENTRE

Potential Data Flow of a MMA connected to an Embedded Insulin Pump



Potential Data Flow of a MMA connected to an Embedded Insulin Pump



Cybersecurity Workshop Objectives

- Offer the fundamentals through practice for security and privacy of MMA data in flow by:
 - Provide a use case MMA data in flow to exercise cybersecurity practice
 - Provide overview of assessing security and privacy requirements for MMA information in flow
 - Applying suitable customised security and privacy controls, Data Flow Security Controls (DFSCs), with an established threat modelling methodology within the use case
- Analyse and compare the use of STRIDE and the Secure Data Flow Framework