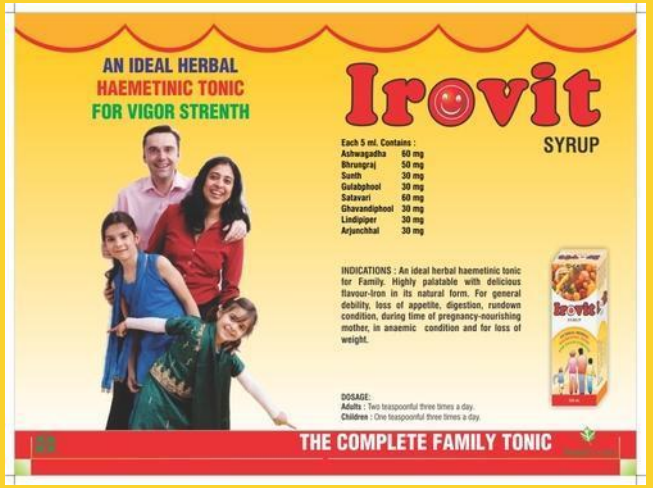
Securing the customer/patient data in an IoT environment

Bodil Josefsson, Head of IoT security

Data privacy and consent. It's a matter of Trust

Increasing privacy regulations and expectations



The network is turning into a platform for business innovation

New contexts and use cases to secure

Growth of potentially unsecure devices

Security & privacy standards & regulations to meet

Security & privacy management challenge

Critical business processes directly impacted

New business contexts → New attack vectors → New security & privacy approach

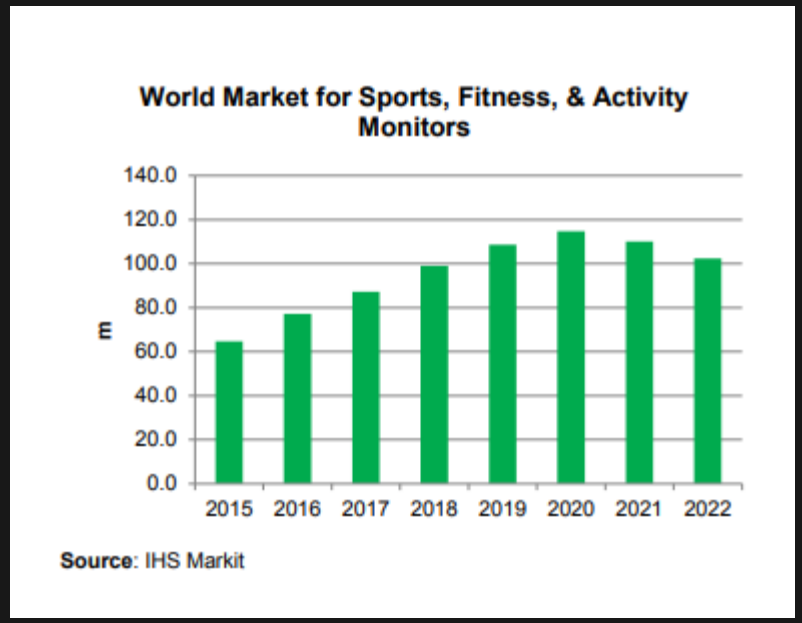
Patients must be able to rely on that IoT is secure

- Secured connectivity
- Trusted devices and identities
- Trusted data integrity
- Privacy and confidentiality
- Confidence that policies are being adhered to

Health devices and wellness devices
- regulated vs non-regulated

Medical IoT device shipments approach 200 million by 2022

Source: "Medical IoT Vertical Market Brief", IHS Markit 2018



Global shipments of sports, fitness and activity monitors will surpass 100 million in 2019

Source: IHS Markit's Sports, Fitness & Activities Monitors Database

E-health transformation is happening everywhere

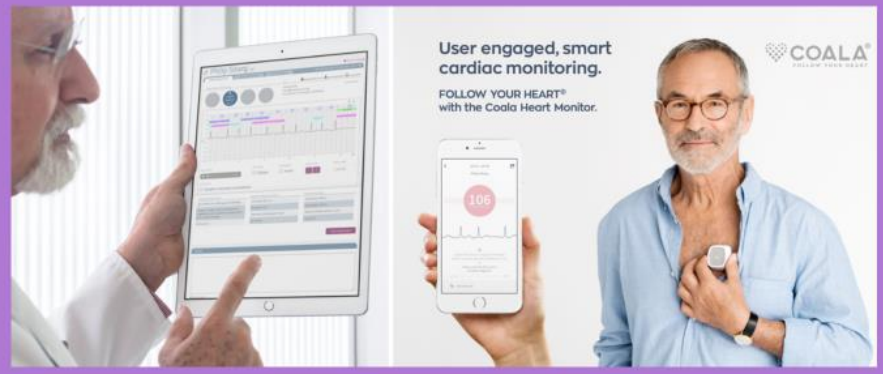
E-Health transformation
Example 1: Remote Patient Care (Jämtland, Sweden)

Service: Remote healthcare stations with video enabled equipment that allows doctor to remotely check up on patient, including finger cameras, ear cameras, etc. In future 5G use cases, same technology could be used in ambulances

Customer Benefits: Faster and more convenient care. Patients do not have to travel to doctor or wait for doctor to visit remote locations.

Healthcare Benefits: Doctors are currently spending 20-40% of their time in a car driving between patients in remote areas.

E-Health transformation
Example 3: Coala Life – a health device for heart monitoring

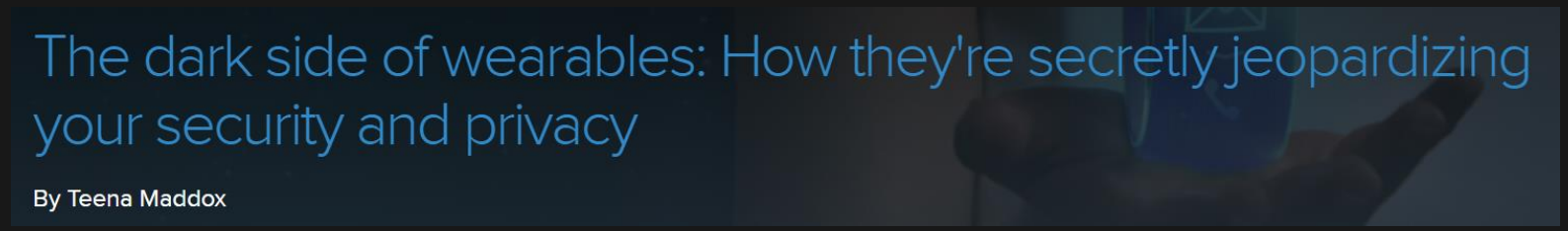


E-Health transformation
Example 2: Remote Patient Monitoring (AT&T, USA)

We see increased security and privacy risks with fitness trackers

Source: Washington Citypaper

Source: CBS Evening News, January 29, 2018



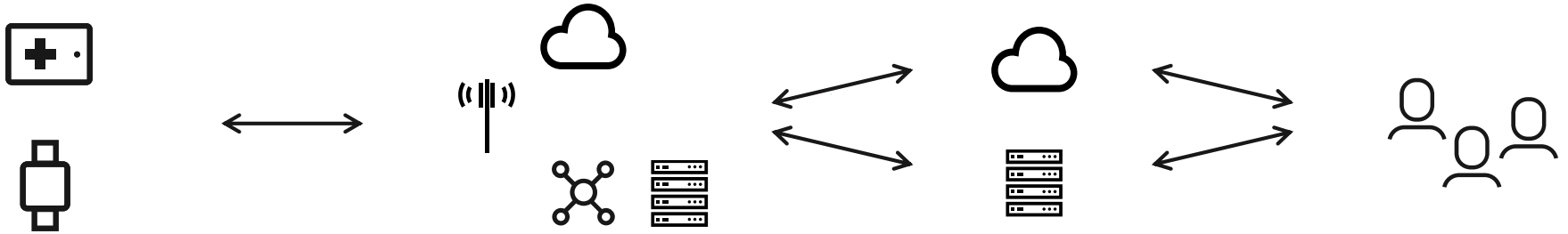
Source: TechRepublic

E2E architecture for security and privacy

Threat Intelligence

End-to-end security management

Devices	Access & connectivity	Applications & cloud	Users



How to detect malicious devices and ensure trusted identities?

Prioritization of vulnerabilities, hardening of network nodes, detection of DDoS attacks

How to detect deficiencies in applications?

How to detect malicious users?

Patient data will come from several sources

Medical records

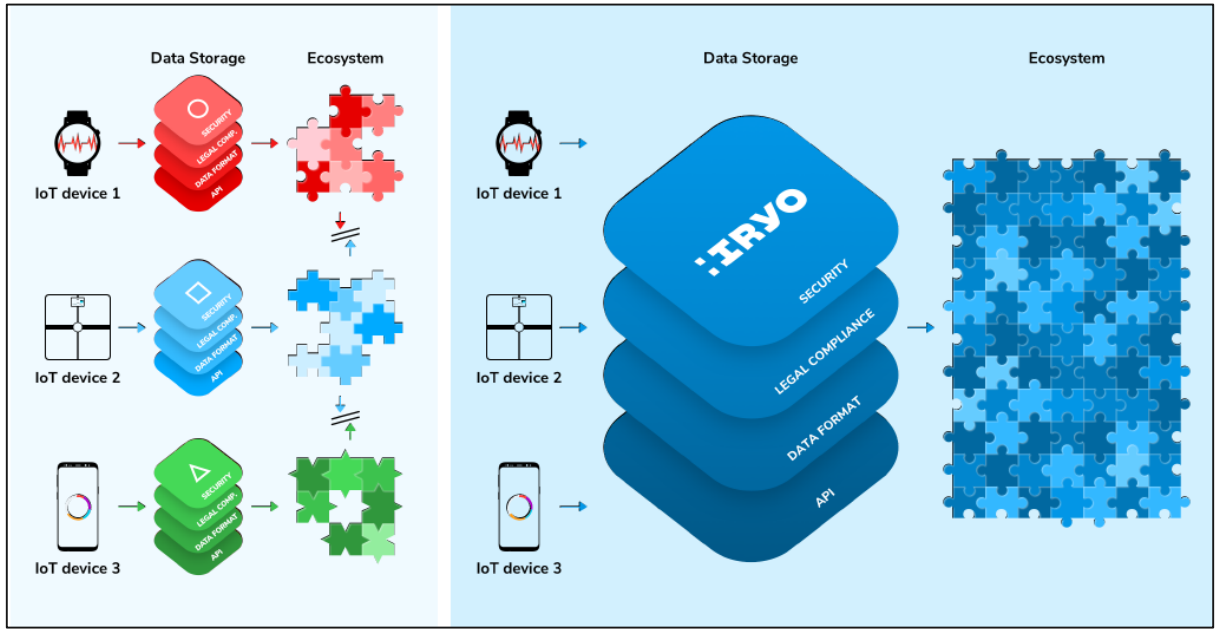
Data from health devices

Data from wellness devices

Aggregated patient data

Zero-knowledge databases
suitable for privacy protection

— User is in control
— Accessed through public-private keys (if the database gets hacked, it will only be raw data. Keys are needed to make sense of data)
— Blockchain technology to ensure data integrity and immutable access control



Authentication trends

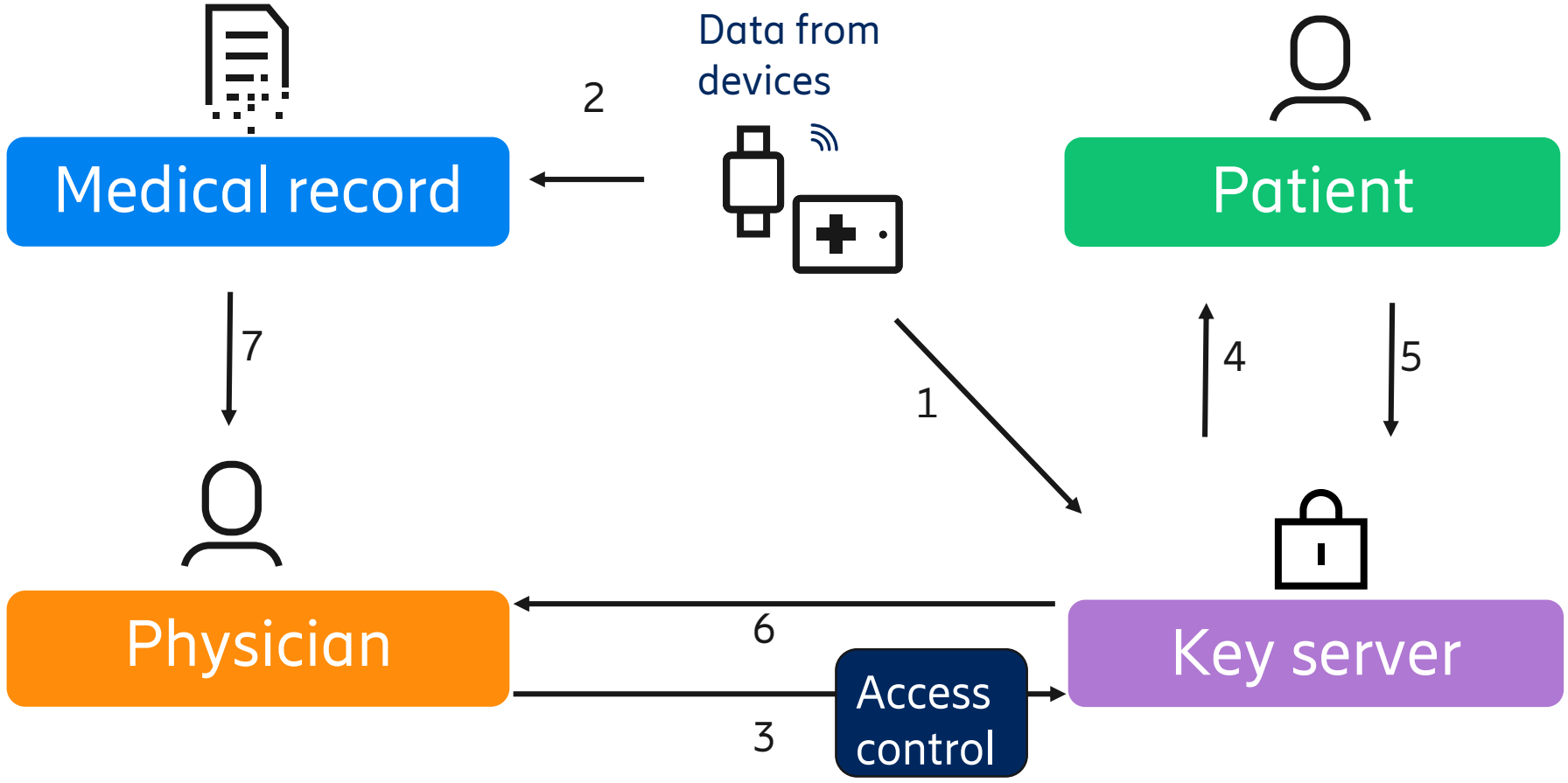
Advanced authentication

Mobile is global

Self-sovereign identity

Telco advantage

The patient (data owner) to be in control of the data



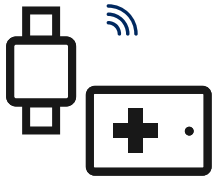
Selective 3rd party disclosure

Medical record

UPLOADED DATA SET

Heart condition monitoring
Exercise records
Weight loss progress, calorie intake

Data from devices

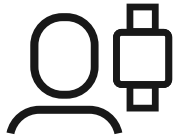


Patient

Physician

Cardiologist

Blood pressure information, weight, activity



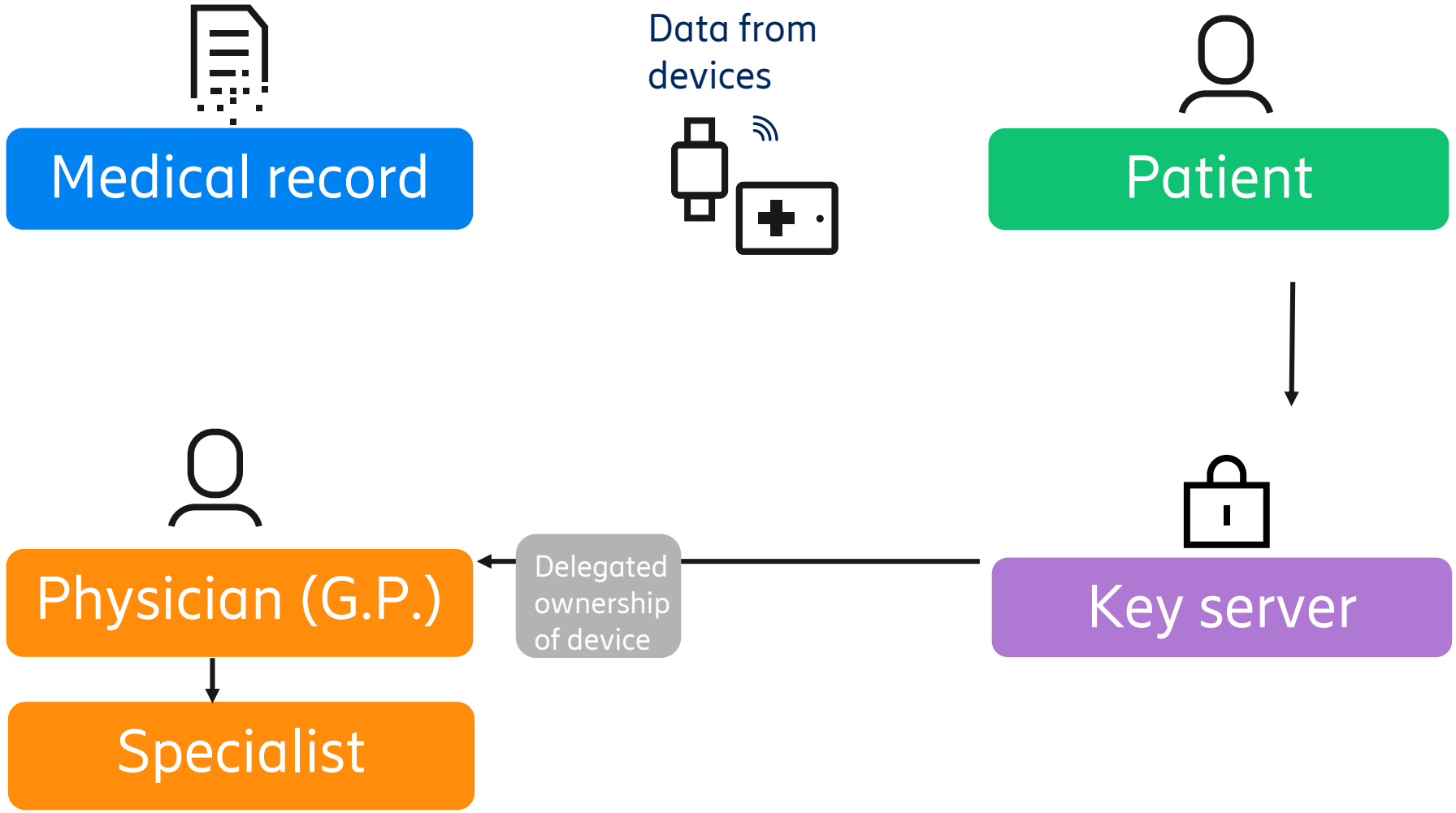
Fitness coach

Activity, food diary

Nutritionist

Food diary, weight

Delegation of a device to a 3rd party



Conclusion

- The introduction of health and wellness devices puts new demands on privacy handling
- E2e security and privacy management is a necessity
- Consent management must be reliable
- Emerging technologies such as AI and Blockchain