PRıVACY AND SECURıTY FOR MOBILE AND CLOUD FRONTIERS IN HEALTHCARE

Ömer KARAYEL
Emre AY
Anıl ÇİÇEK

CONTENTS

- The benefits of healthcare IT
- Needs of healthcare
- Critical Research Challenges
- Conclusion

INFORMATıON TECHNOLOGıES ıN HEALTHCARE

- Information technology (IT) has great potential to improve healthcare
- Health care industry will invest $5.4 Billion in Cloud Computing by 2017.
- Increasing use of mobile devices, cloud services and EHR

WHY THE HEALTHCARE SECTOR IS GENERALLY SLOW TO ADOPT

“Healthcare industry moves toward automation and online records, yet falls behind when addressing *security and privacy*, ranking below retail in terms of cybersecurity”

Other critical issues include data availability, error limitations, disaster backup and rapid response times

NEEDS OF HEALTHCARE SECTORS

- Access to right information
- High accuracy
- Higher level interaction
- Secure Data storage and Access
- Reduce IT cost

ADVANTAGES OF ıNFORMATION TECHNOLOGY IN HEALTHCARE

- Users have unlimited access to the software using any device connected to the Internet
- Data can be shared with other systems
- All users access the same version of the software
- Maintenance and upgrades to newer versions are easier
- Any Time Any where service
- Health care data security are improving
- The system has its own IT support; and

  Investment in application or database management is unnecessary

SUMMARY

—The benefits of healthcare IT will be elusive if its security challenges are not adequately addressed

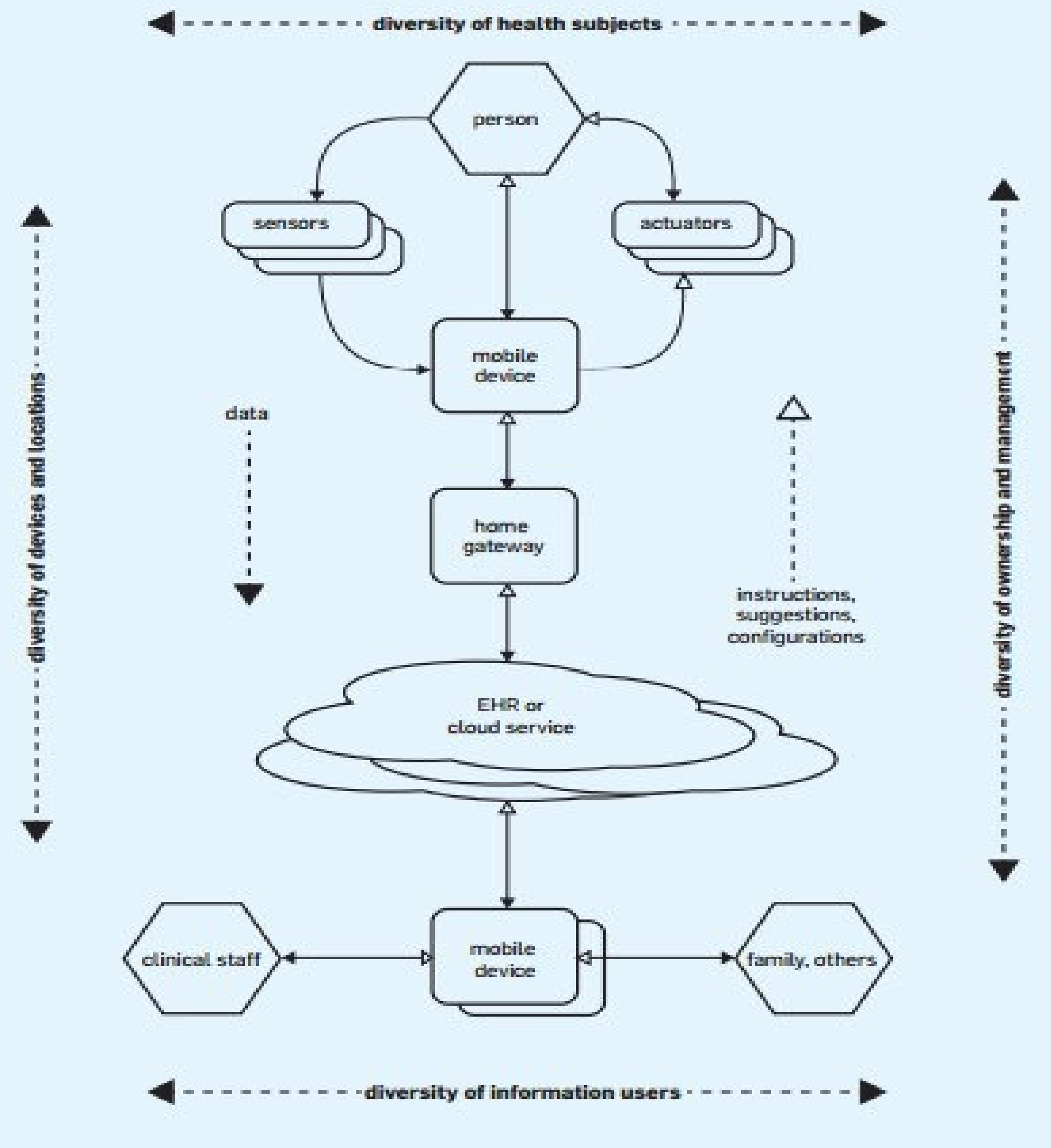
—More than two-thirds (69%) of respondents say their organization’s IT security does not meet expectations for FDA-approved medical devices.

—Privacy protection is also critical for healthcare IT; although this column focuses on security, it should be noted that many security breaches lead to disclosure of personal information and thus an impact on patient privacy

CRITICAL RESEARCH CHALLENGES

- Usable authentication tools
- Trustworthy control of medical devices
- Trust through accountability

The complex trust relationships involved in healthcare information technologies.



diversity of health subjects
person
sensors
actuators
mobile device
data
home gateway
instructions, suggestions, configurations
EHR or cloud service
clinical staff
mobile device
family, others
diversity of devices and locations
diversity of ownership and management
diversity of information users

INFORMATION TECHNOLOGIES IN HEALTHCARE

- Those who use medical information are diverse: families, clinicians, researchers, insurers and employers are some examples.

- Those who provide information is also diverse: traditional patients, healthy athletes, children, elderly and so forth.

- The mobile devices and systems are also diverse. The result is a complex mix of thrust relationships.

USABLE AUTHENTICATION TOOLS

- Traditional authentication mechanisms like passwords can disrupt workflow and interfere with the primary mission of patient care.
- Recognize that staff often wear gloves and masks.
- EHR systems should not arbitrarily limit clinical staff from viewing an entire record. Denying access in an emergency situation may lead to delayed care or even death.
- However devices should provide needed information without too much information and trigger automated systems.

TRUSTWORTHY CONTROL OF MEDICAL DEVICES

- Today’s sophisticated medical devices like infusion pumps and vitalsign monitors are increasingly networked and run safety-critical software.

- Networkcapable medical devices may have cyber-security vulnerabilities that can have implications for patient safety.

- Medical devices must contain defenses against today’s known vulnerabilities and tomorrow’s anticipated threats.

TRUSTWORTHY CONTROL OF MEDICAL DEVICES

- Conficker and botnet malware can break into unmaintained systems easily; old operating systems provide large reservoirs for the Conficker worm, and medical devices can have long product life cycles that persist with outdated operating system software.

TRUST THROUGH ACCOUNTABILITY

- Health IT provides a foundation for diagnosis, treatment, and other medical decision making.
- This foundation must be both dependable and trustworthy.
- Health IT must be accountable, which means people and organizations must be held responsible for the ways the systems are used.

TRUST THROUGH ACCOUNTABILITY

- Audit logs of all IT systems are needed to monitor buggy or inappropriate behaviours.

- Automated analysis of audit logs in medical systems would be useful, as would be the ability to detect anomalies.

- Access restrictions should be imposed according to workflow data and/or models trained via machine learning to diminish reliance on post-hoc accountability.

SECURITY

Transmission and storage of information is very easy with cloud computing sector but this sector has security problems. The theft of people’s health problem informations have great risks.

EXAMPLES

Apple suffered a loss of confidence for hacking incidents in 2014.Stolen informations of users spread on the internet. At the end of 2014 apple was a drop in sales.

EXAMPLES

- After this hacking incidents Hackers steal details of the company’s employees , movies and correspondences from Sony. Sony in trouble for this stolen informations. Some institutions sue to Sony.

IF THIS SECTOR HACKED

- If we use the cloud computing in mobil health this is very easy but if hackers steal this informations ; people’s healt problems ,required medicines or weakness of society revealed.

IF THIS SECTOR HACKED

- No country no state dont want to experience like this situation . If this informations stolen from hackers this is very bad situation for national defense. Thats why investments are made by the mobile health governments create a cyber defense shield in this status.

CONCLUSıON

- If we want to develop this sector clients must know their personel informations in safe. Produced solutions for this is suitable and useful to the workflow of doctors and nurses.In this way we can access right technic and enough security level.