Health data security and privacy

Michael Stefanoudakis, George Iakovakis

stefanoydakis@gmail.com, giakovakis@aueb.gr

Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory

Dept. of Informatics, Athens University of Economics & Business (AUEB), Greece

Introduction

eHealth is the use of Information and Communication Technologies (ICTs) for health and integrates a bunch of ICTs. ICTs integration challenges, including different medical technologies, combined with the requirement to share information between newly merged organizations creating new vulnerabilities. The scope of this research is to expand on security and privacy issues in the eHealth sector. In particular, we will explore the current situation in Europe and Greece regarding the implementation of security legislation and policies. We focus on cybersecurity measures and solutions in the eHealth sector and more specifically we try to analyze technical measures, eHealth security measures and solutions to defend against threats.

Definitions

In order to comprehend the main section of our results it is vital to explain the next definitions:

- ***mHealth***: The use of mobile devices – such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and wireless devices – for medical and public health practice [1].
- ***Telehealth:*** Delivery of health care services, where patients and providers are separated by distance. Telehealth uses ICTs for the exchange of information for the diagnosis and treatment of diseases and injuries, research, and evaluation, and for the continuing education of health professionals [1].
- ***Personal Health Record (PHR):*** a computerized health record created and maintained by an individual who is proactive in the management of her or his own health. The record can be private or made available to health-care providers. PHRs can store a diverse range of information such as an individual's allergies, adverse drug reactions, chronic diseases, family history, illnesses and hospitalizations, medications, diet and exercise plans, and test results [2].

eHealth Specific Issues on Security and Privacy

eHealth improves and innovates the operations, the quality and the financial efficiency of the healthcare sector using ICTs that support the eHealth services and management of their system components. The NIS Directive defines as health subsectors, health care settings, including hospitals and private clinics that offer their services outside of their environment, as shown in ***Figure 1.***

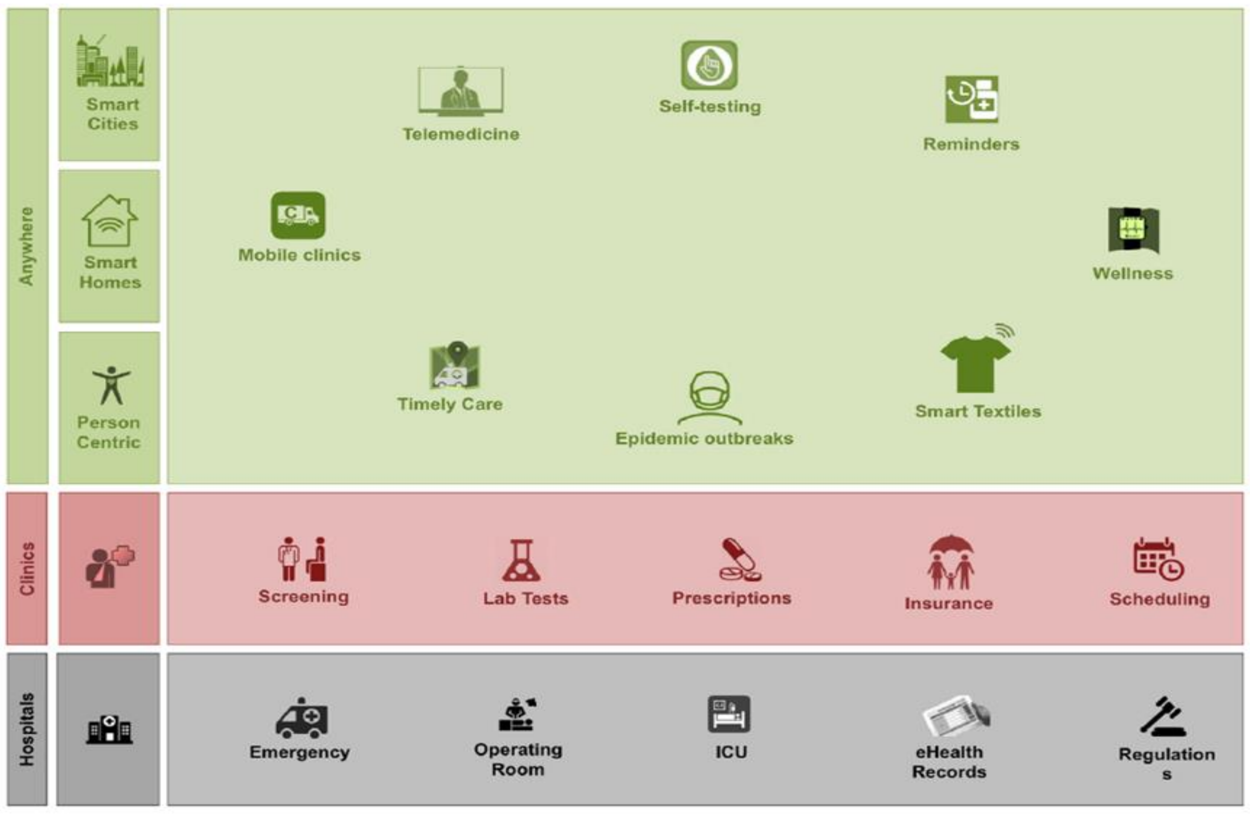

Figure 1: *eHealth services in the context of stakeholders, operations, and application.[3]*

Common Cyber Threats in eHealth

In our research, we analyze threats which are prevalent in the eHealth sector such as social engineering and phishing (which have as primary attack vector the email), ransomware, device and data theft, data loss caused by human errors and insiders and medical device tampering, as depicted simply by ***Figure 2.***

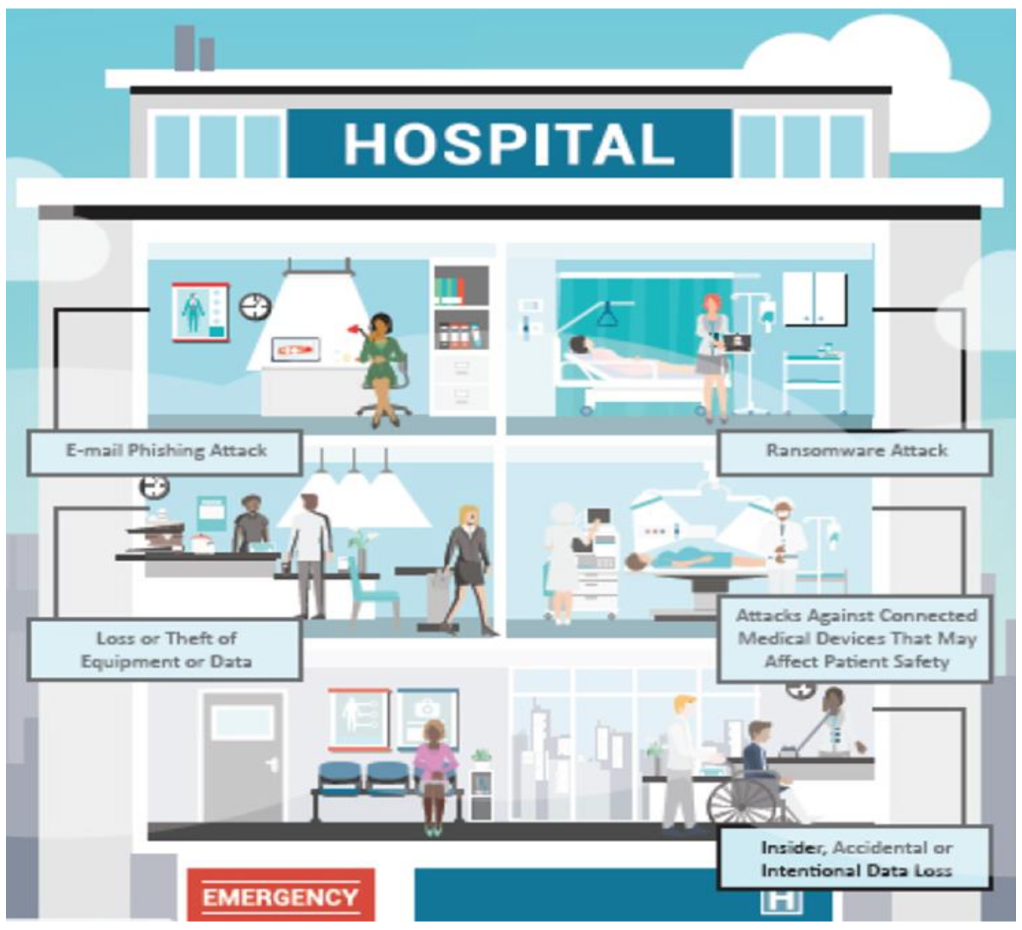
HOSPITAL
E-mail Phishing Attack
Ransomware Attack
Loss or Theft of Equipment or Data
Attacks Against Connected Medical Devices That May Affect Patient Safety
Insider, Accidental or Intentional Data Loss
EMERGENCY

Figure 2: *The most prevalent attacks in a healthcare organization. [4]*

Security Guidelines Related to eHealth

Guidelines provide good practices, such as the recommendation of security measures, and giving directions for choosing the appropriate cybersecurity solutions to implement these measures. After research and analysis, we identify the following resources that provide concrete and useful information on eHealth cybersecurity:

- Email protection
- Endpoint protection
- Identity Management and Access Control
- Data Protection and Loss Prevention
- Asset Management
- Network Management
- Vulnerability Management

Conclusions

The health sector was recognized by the EU through the NIS directive as a critical sector [5], so, we should always keep in mind that the majority of eHealth services are critical and therefore the eHealth infrastructure that supports them is critical, too. Healthcare organizations must take additional steps to achieve security requirements by implementing stronger defenses and good practices which means applying a collection of security solutions to prevent any attraction from threat actors, as it turned out during the COVID-19 pandemic and the crisis that followed. The COVID-19 crisis has made the need for prevention urgent and the lessons that humanity has learned are hopefully enough to highlight the role of security and privacy in the whole eHealth ecosystem.

References

1. World Health Organization, "Global diffusion of eHealth: Making universal health coverage achievable," Report of the third global survey on eHealth Global Observatory for eHealth, 2016. [Online]. Available: http://who.int/goe/publications/global_diffusion/en/
2. World Health Organization, "National eHealth Strategy Toolkit," 2012. [Online]. Available: https://www.who.int/ehealth/publications/en/
3. Farahani B., Firouzi F., Chang V., Badaroglu M., Constant N., and Mankodiya K., "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," Futur. Gener. Comput. Syst., vol. 78, pp. 659–676, 2018.
4. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)," Cybersecurity Act of 2015, Section 405(d) Task Group. [Online]. Available: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf
5. European Parliament, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union." [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
6. Rahmani et al., "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," Futur. Gener. Comput. Syst., vol. 78, pp. 641–658, 2018.
7. Wang X. and Jin Z., "An Overview of Mobile Cloud Computing for Pervasive Healthcare," IEEE Access, vol. 7, pp. 66774–66791, 2019.
8. Abouelmehdi K., Beni-Hessane A., and Khaloufi H., "Big healthcare data: preserving security and privacy," J. Big Data, vol. 5, no. 1, pp. 1–18, 2018.
9. Dhanvijay M. and Patil S., "Internet of Things: A survey of enabling technologies in healthcare and its applications," Comput. Networks, vol. 153, pp. 113–131, 2019.
10. National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity." [Online]. Available: https://www.nist.gov/cyberframework/framework. [Accessed: 17-Jul-2020].
11. Dritsas S., Tsoumas B., Dritsou V., Konstantopoulos P., Gritzalis D., "OntoSPIT: SPIT Management through Ontologies", Computer Communications, Vol. 32, No. 2, pp. 203 -212, 2009.
12. Kotzanikolaou P., Theocharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection (CIP-2013), pp. 171-182, Springer (AICT 417), USA, March 2013..
13. Gritzalis D., Iseppi G., Mylonas A., Stavrou V., "Exiting the risk assessment maze: A meta-survey", ACM Computing Surveys, Vol. 51, No. 1, pp. 11.1-11.30, January 2018.
14. Virvilis N., Gritzalis D., "The Big Four - What we did wrong in Advanced Persistent Threat detection?", in Proc. of the 8th International Conference on Availability, Reliability & Security, pp. 248-254, IEEE Press, Germany, 2013.
15. Virvilis N., Gritzalis D., "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", in Proc. of 10th IEEE International Conference on Autonomic and Trusted Computing, pp. 396-403, IEEE Press, Italy, 2013.