SHAPES Cyber Secure HealthCare Platform in Digital Environments

JYRI RAJAMÄKI
Leppävaara Campus
Laurea University of Applied Sciences
Vanha maantie 9, 02650 Espoo
FINLAND
jyri.rajamaki@laurea.fi https://www.laurea.fi/en/

Abstract: - The SHAPES project is an ambitious endeavor that gathers stakeholders from across Europe to create, deploy and pilot at large-scale a EU-standardized open platform incorporating and integrating a broad range of solutions, including technological, organizational, clinical, educational and societal, to enable the ageing population of Europe to remain healthy, active and productive, as well as to maintain a high quality of life and sense of wellbeing for the longest time possible. The research question of this design science research (DSR) is how to build and deploy health and care (H&C) services into a future society in such a way that citizens are able to use them safely in their every day lives? We found that considerable work is needed to develop the required architecture in smart societies: information architecture, integrations architecture, target architecture, security architecture, and security issues. Service chains must be checked against the architectures to ensure no risks are present.

Key-Words: - cloud services, cross-border healthcare, eHealth, healthy aging, SHAPES project, well-being

Received: May 18, 2019. Revised: December 26, 2019. Accepted: January 23, 2020. Published: February 4, 2020.

1 Introduction

The use of information and communication technology (ICT) in health and care (H&C) sector has increased due to the potential improvements in effectiveness and efficiency. Digital transformation and ecosystem thinking steer the Smart and Healthy Ageing through People Engaging in Supportive Systems (SHAPES) project [1] that supports the well-being of the elderly at home.

This design science research (DSR) tries to be a step towards new meta-artifacts and useful methods for the design and validation of cyber-security requirements engineering approaches into digital H&C systems and services. Figure 1 presents this study's DSR framework.

The Relevance Cycle of DSR bridges the contextual environment of the research project with the design science activities [2]. Within eHealth Domain, the Environment includes people (e.g. citizens as patients and taxpayers, healthcare professionals), organizational systems (e.g. public and private H&C service providers, drug manufacturers, payers such as Medicare, Medicaid, insurance companies, HMOs), technical systems (e.g. ICT, IoT, AI, robotics) and different related problems (e.g. availability, integrity and confidentiality of information in eHealth systems). The Rigor Cycle connects the design science activities with the Knowledge Base of scientific foundations, experience, and expertise that informs the research project [2]. The knowledge base of this study consists of Enterprise Architecture (EA). The central Design Cycle iterates between the core

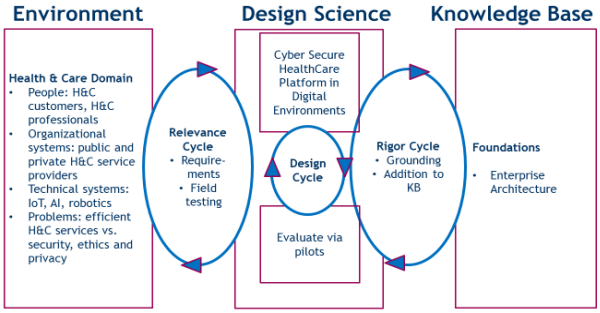

Fig.1 Design Science Research framework of the study (modified from [2])

2 eHealth Environment

The H&C sector is becoming increasingly complex. Day by day, hospitals are increasing the digital transformation using in an extensive way more digital and communications technologies. With a society getting older and older, the search for technological solutions in the field of health to

reduce operational costs has become a necessity within the European economic sphere. Thanks to ICT, most of the traditional services are being digitized which means a cost reduction and at the same time allows coverage of a larger number of people, increasing the performance. But, on the other hand, it opens the healthcare system to the attacks of anyone. In order to detect and to remedy the cyberattacks, it is needed to deploy Managed Security Services, which will allow to detect, analyze, notify and solve any security incident in the network or devices of the Hospital Center staff through an expert team of professionals and through a network of SOCs (Security Operation Centers). This service enables end-to-end security management offering the maximum levels of security, guaranteeing operational continuity and reducing costs derived from attacks and inefficiencies by incorporating the latest advances in protection without the need for new investments or internal developments.

Cloud computing and big data have emerged as important disruptive technologies that influence H&C research communities [3]. The Internet of Things (IoT) is an emerging trend, which provides a substantial amount of efficient and effective services for patients as well as H&C professionals for the treatment of various diseases [4]. In addition, assistive robots, eHealth sensors and wearables, and mobile applications (Apps) get increasingly common in H&C sector. However, privacy concerns pose a major challenge in the widespread use of these practices in H&C [4] [3]. In many cases, H&C metadata contains privacy-sensitive information about individuals and publishing this data could violate the principles of individual privacy [3]. On the other hand, integrity and availability of the patient information are vital from the point of view of the patients' safe care.

The design challenges in digital H&C services stem from the fact that there are multiple stakeholders whose interests have to be met: 1) physicians who often are not willing to learn or adopt new ICT systems; 2) payers (Medicare/ Medicaid, insurance companies, health maintenance organizations) who need to review billing claims; 3) drug manufacturers who need access to clinical data; 4) medical device original equipment manufacturers also need to view data; and 5) the patients who would like to control our own medical data in a secured manner [2].

2.1 Security Aspects in eHealth

The digital security of information is traditionally expressed in terms of maintaining three characteristics of the information: confidentiality, integrity and availability. In addressing the provision of data security services for information assets, it is necessary to consider the state of the information: is it in storage, in transmission, or in use as being processed. When considering possible aspects to secure digital information, three classes occur: technological solutions; policy-regulation; and practices related to information management; and the frames of education and situational awareness as views of all stakeholders in the security implications of potential activities. The three characteristics of information, the three states of information and three classes of security aspects form the basis of an information security-resilience frame exists, confer [5] and our furthered Figure 2.

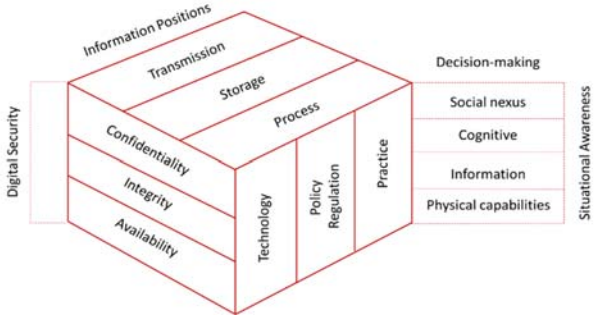

Fig.2 Security Aspects for Information Dimensions (modified from [5])

Digital security is generally understood as a 'weakest link' problem, so the system cannot be considered secure unless all aspects are dealt with adequately, and with regard to eHealth, many people consider this unlikely to be achieved, hence, the continuing concerns over information privacy [6]. On the other hand, others consider eHealth systems an opportunity to achieve better security and privacy protection than what is available in paper-based systems through additional security functionalities: user authentications and authorizations, the retention of back-up files, user defined storage and retrievals and accountability measures, monitoring and logging access to records, and establishing audit trails and other mechanisms to enable information accountability [6]. However, these require a more comprehensive approach than an attempt to add on technological security measures to an incompletely specified eHealth system.

2.2 Cybersecurity Challenges in eHealth

In 2015, The European Union Agency for Network and Information Security (ENISA) published their study "Security and Resilience in eHealth" [7] that focus on eHealth information systems and infrastructures as well as on the relevant assets that are considered critical both for the society and the relevant stakeholder groups. This study can be seen as a description of the state of the art how EU member states perceive cybersecurity in their health systems, which are the specific approaches they follow, and which are the measures they take to protect these systems.

According to the ENISA, the most important cybersecurity challenges in eHealth infrastructures and systems are: 1) systems availability; 2) lack of interoperability; 3) access control and authentication; 4) data integrity; 5) network security; 6) security expertise and awareness; 7) data loss; 8) standardization, compliance and trust; 9) cross-border incidents; and 10) incidents management [7].

3 Enterprise architecture

Enterprise architecture (EA) is an effective way to implement the architecture of smart eHealth systems, both now and in the future. Through EA, we can develop strategies based on visions and scenarios. It provides the methods and tools, and a consistent approach to the smart cities` functions and enables the practical implementation of strategies [8].

Both our objectives and the driving forces of change are better understood when approached through future visions, scenarios, and descriptions of targets, and in this way, the smart eHealth systems can be described with the necessary accuracy. The necessary constraints and changes to the architectures are determined by analyzing the status, future visions, and scenarios and dependencies, from which we can also define cyber threats and risks. When developmental work is implemented efficiently through architectural guidance (EA), the benefits of the developments can be maximized [9].

EA supports systems management, strategy implementation, the continuous development of operations and services, change management, complexity management, and the orderly use and interoperability of digitalization [8]. In this way, it also helps us better understand virtualization functionality and the architectural work required in future communications and service environments, as well as data centers. EA should be a part of the strategic work of the organization, its work and management processes, and its economic and operational planning.

EA can be accomplished in many ways; it can take into account things in different ways, have different visions and strategies, be at different stages of development, and incorporate systems at different life cycle stages, etc. Through the guidance of EA, we can enable smart eHealth systems to function properly and provide their citizens with the necessary services, and to pursue development in all areas and in all segments in the future. Figure 3 shows one example of an EA Framework.

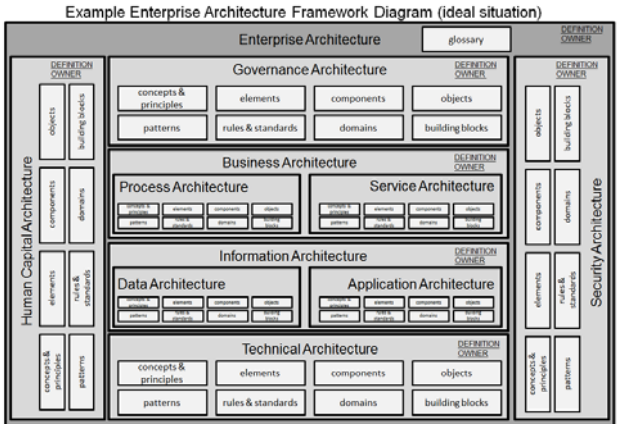

Fig.3 Example of the Enterprise Architecture Framework Diagram (modified from [10])

When social services are integrated into a virtualized network and service environment, co-operative approaches and same type of solutions, as well as use cases, will be increasingly important in order to develop the services of the future. When considering security, cybersecurity, and privacy, these issues need to be examined from all segments and from inside the segments, as well as through virtualized solutions between different virtual operators' networks, and services between different security levels, because they are working in the same environments and are using the same infrastructures [9]. In future, where everything is connected to everything, services at different security levels are offered on the same network and on the same service platforms. This also means that we need new types of smart user devices, with which we can address that environment`s requirements and functionalities [11], [12].

At the same time, these connections and solutions are used by less critical services, or other intelligent social services. The implementation of cybersecurity and security in this type of environment is a challenge for everyone. This

requires a variety of Intelligent Data Management Platform (IIMP) systems to manage the flow of information in intelligent cities and in a smart society, within and between countries, and in the exchange of information between continents [13].

When consider the main points of digitalization, we will also want as many potential activities as possible, which are automatically implemented in the background so that we do not even notice them. This requires substantial changes in the way things have been done in the past. It is not sufficient for one agency or one organisation to take care of all architectural activities from start to finish. While we use EA and its framework to make architectures for smart eHealth systems, high-level cooperation and coordination is needed [9]. However, digitalization is only one aspect of smart eHealth systems that needs to be considered and explored.
Communications and services are also benefitting from other technical advances that will change much in future communication and service solutions and platforms [9].

Information (data) has achieved a key role in smart eHealth systems. However, information is no longer understood only as part of the information system, not as a stand-alone and separate entity, and in many places, it is part of infrastructures and other smart structures. One of the guiding principles is that also proposed at the EU level: "Request information only once". EA can also provide tools and procedures to help develop systems in these cases [9].

4 Design Targets

The integration of a broad range of technological, organizational, clinical, educational and societal solutions seeks to facilitate long-term healthy and active ageing and the maintenance of a high-quality standard of life. Mediated by technology, in-home and local community environments interact with H&C networks contributing to the reduction of H&C costs, hospitalizations and institutional care. This section looks at the overall research question - *how to build and deploy H&C services into a future society in such a way that citizens are able to use them safely in their everyday lives* - from four different design target's point of view.

4.1 From Hospitals to Home

Europe is ageing. Good health is not only of value to the individual as a major determinant of quality of life, well-being and social participation; it contributes to general social and economic growth [8]. Accessibility to healthcare is thus one of the key priorities of the EU health policy. Integrated care focuses on the needs of the recipient on coordination between diagnosis and treatment and between primary care and secondary care, and between different therapeutic areas and specialties. Benefits of integrated care models are clear; still, the complexity of healthcare systems in individual countries and regions adds to the challenge. The redesign requires shifting care from hospitals to home. While individuals with chronic conditions need regular care and/or support that can often be delivered at home by community nurses, or others, potentially using information and communication technologies. Regular, reliable homecare ensures changes in the condition and treatment, resulting in better-managed conditions and fewer hospitalizations. New digital solutions include assistive robots, eHealth sensors and wearables, Internet of Things (IoT)-enabled devices and mobile applications. Cyber security is a prerequisite for the launch of these services.

Figure 4 shows the process of Intelligent Information Management for eHealth environments and it gives possibilities of how to follow and verify that patient sensor and IoT device data are going to the right place and are accessible only by authorized healthcare individuals. A system called 'IIMP' monitors patients' IoT-devices and sensors' information flow to hospital healthcare systems to provide healthcare personnel with a rapid analysis of the information. IIMP ensures that medical staff can find information about patients even in critical situations. This type of system can also help to find anomalies or data changes, or identify if someone has attempted to penetrate or use data in an undesirable way. The user can create specific action groups for this system. Members of the user group can follow the progress and changes of situations, data resources and reports in real time.

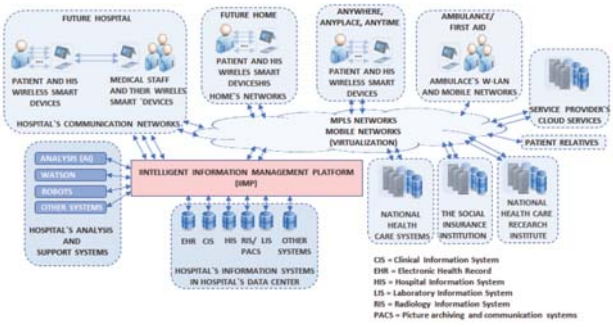

Fig.4 eHealth operating environment [9]

SHAPES leverages the outcomes of an open interoperability framework symbIoT [10] that empowers the interconnection of different IoT-based platforms, devices, digital solutions and services. symbIoT middleware supports controlled and secure exchange of information, sharing of resources and best practices and delivering of services to third-parties, thus enabling the building of a true ecosystem of digital solutions and services that may be selected and tailored to the specific individuals' needs, interests and contextual environment, fostering SHAPES' large-scale pan-European deployment and market scale-up. symbIoTe including open software development kits and application programming interfaces provides an interoperable mediation framework that enables the discovery and sharing of connected devices across existing and future IoT-platforms for development of cross-platform IoT-applications.

4.2 Authentication and Security Assessment as a Service in SHAPES

SHAPES manages a high degree of sensitive information pertaining to older individuals thus it is critical that high standards for security and privacy (fully adopting GDPR) are implemented, resulting in a trusted platform among its users and stakeholders. User authentication considers mechanisms that are seamless, noticing that seniors may lack technological skills or have unreliable memory to recall strong passwords. So, SHAPES implements user authentication mechanisms based on Multimodal Biometrics using several physiological or behavioral human characteristic for enrolment, verification, authentication or identification. SHAPES demonstrates capabilities (face recognition and fingerprint) applying multi-factor authentication in a seamless way. Concerning device and component authentication, SHAPES brings a twofold approach:

SHAPES implements an authentication mechanism that is able to take into consideration state-of-the-art protocols (end-to-end encryption, PKI, web-based using secure API call and token-based authentication) and IoT-friendly lightweight protocols, such as the Constrained Application Protocol (CoAP) for message exchanges. Most IoT-devices allow re-use of existing Enrolment over Secure Transport (EST) functionality for energy-efficient certification management and secure bootstrapping operations.

SHAPES implements a state-of-the-art authentication mechanism based on secure stateless tokens 'Paseto' (Platform -Agnostic SEcurity Tokens) that enables a distributed mechanism for token-based authentication achieving inter-module authentication.

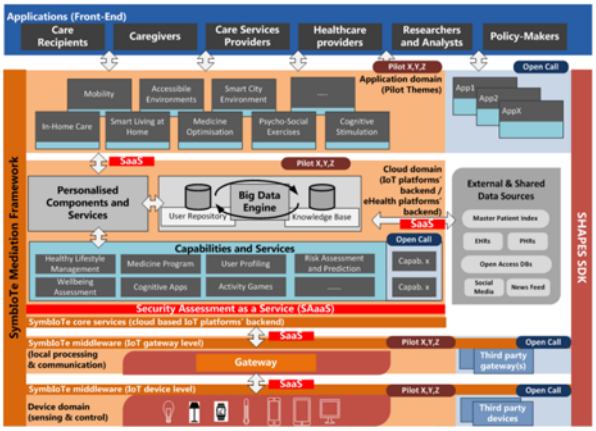

Fig.5 SHAPES high level architecture [11]

Considering the likelihood of operating in a not secured environment, SHAPES creates over-the-top secure environment (Virtual Local Area Network) enforcing security best practices. Moreover, it integrates a Security Assessment as a Service (SAaaS) cross-layered system to dynamically detect any existing and newly introduced network device, perform vulnerability assessments, certify the device against a standardized CVSS, assign it to a connectivity-appropriate VLAN and authenticate the service or device. Figure 5 presents SHAPES' high-level diagram.

4.3 Empowering

Health literacy, technology and individual involvement in care make healthcare more user-friendly and empowering, meaning that citizens (including seniors) must be seen as custodians of their own health [12]. Citizens continue to take a more central role in decisions about their own healthcare, and new technologies enable and facilitate this trend. New patients are evolving, similar to retail consumers. These former patients – new healthcare consumers – are driven by desire to take control over own health records and want to take active part in choosing healthcare providers and services. They are driven by the desire for more trustworthy, secure and timely healthcare information. Due to this changing role of patients, their empowerment has become a key priority for policy makers, professionals and service providers. Citizens' role is transforming from passive receivers

of healthcare to active decision-makers; and managing own health data. Security is important aspect to empowering and creating the trust [13].

As an example, activity-trackers enable to collect data from individuals' physical activities and health. A qualitative study [14] regarding the user perception on the privacy and sensitivity of health information collected with activity-tracker explored the user perception on health information sensitivity in general, and their willingness to share such information to other parties. Laufer and Wolfe's [15] privacy calculus model modified by Dinev and Hart [16] was the theory throughout the study. Table 1 summarize the results. Individuals do not perceive the information collected by activity-trackers as private or sensitive. On the other hand, information in medical records is considered to be very sensitive and private, as they include text written by doctors about procedures and discussions that are considered to be the most sensitive type of information.

Table 1 Research findings from activity tracker users' study [14]

Perceived privacy risks	**Perceived privacy concerns**	**Willingness to provide personal health data**
Information stolen	Being tracked or followed	Not on social media
Information lost	Banks deny loan applications	For medical research
Information misused	Employers won't hire	For healthcare purposes
Information goes to third parties	Insurance companies deny payments	For improving wearable products and services
Unauthorized access to the information	Information used for marketing	For occupational health services

The study extends earlier study information by presenting a new context to utilize the Privacy Calculus theory. The study's benefit is knowledge that activity-trackers users are ready to share their information that can be utilized in research and development of public services.

4.4 Cross-border Healthcare

The EU Directive on the Application of Patients' Rights in Cross-Border Healthcare is a starting point, delivering a legal framework for individuals willing to gain greater access to information related to healthcare available across Europe. However, in order to secure above-mentioned rights and unleash the potential of cross-border healthcare exchange, new solutions are needed to secure the storage and cross-border exchange of health data.

SHAPES cross-border implementation will be in line with modular strategy and related specifications and initiatives of epSOS (Smart Open Services for European Patients) project. In addition to the epSOS, the related and furthered projects are:

1) OpenNCP (Open Source Components for National Contact Points) as base realization starting point for SHAPES which includes a novel framework to foster cross-border eHealth services and which is base into the epSOS specifications;

2) current DECIPHER project which creates a mobile health care solutions and enables secure cross-border access to existing patient healthcare portals; and

3) STORK (Secure idenTity acrOss borders linked) which establishes a European eID Interoperability Platform that will enable citizens and businesses to use their national electronic identities in any participant Member State for public eGovernment services.

The designed contribution is that SHAPES can improve security and resiliency elements to related mechanisms and transactions, which are already established in the related projects.

Based on technological, integration and system readiness levels [17], SHAPES should develop new security readiness level (SecRL) metrics that supports the development of European operational standards for secure cross-border data exchange and patient privacy protection. Based on these metrics and prior open-source solutions (such as the OpenNCP suite [18]), SHAPES could realise secure node platforms and components that enables the secure sharing and exchange of eHealth related data among countries.

5. Discussion and Conclusions

The rights of ageing individuals and their ability to live a good life at home or in a home-like environment are at the heart of the services designed in the SHAPES project. Privacy and security competence play a key role in the project, from planning to implementation and assessment. However, according to an ongoing ECHO Horizon 2020 cybersecurity project [24], health care sector can be identified as the most far from the ideal cybersecurity situation.

The future complex environments present many challenges because the standards are not yet set at the international level. IoT products and sensors are

mainly used at proprietary -based standards and getting them work at th e same platforms in the smart devices will be a really big challenge.

The overall cybersecurity work with regard to the SHAPES project consist of two p arts: 1) The SHAPES integrated care platfor m should be secure, and 2) tools for ensuring that SHAPES digital solutions via platform ar e cyber-secure. Considerable work is needed to develop the required architecture in smart eHealth systems and services: information architecture, integrations architecture, target architecture, security architecture, and security issues. Service chains must be checked against the architectures to ensure no risks are present.

Acknowledgements

This work was supported by the SHAPES project, which has received funding from the European Union's Horizon 2020 resear ch and innovation programme under the grant agreement no. 857159.

References:

[1] European Commission, "Smart and healthy ageing through people engaging in su pportive systems," 2019, [Online]. Available: https://cordis.europa.eu/project/id/857159.

[2] A. Hevner and S. Chatte rjee, Design research in information systems: Theory and practice, New York: Springer Science and Business Media, 2010.

[3] K. Mireku, Z. FengLi and K. P. Kibiwott, "A Hybrid Privacy Preservation Framewo rk for Healthcare Data Publishing," American Journal of Engineering Research, vol. 6, no. 7, pp. 173-180.

[4] S. Amaraweera and M. Halgam uge, "Internet of Things in the HealthcareSector: Overview of Security and Privacy Issues," in Security, Privacy and Trust in the IoT Envir onment, Cham, Springer Nature, 2019, pp. 153-180.

[5] "National Training Stand ard for Info rmation Systems Security (INFOSEC) Professionals," NSTISSI, 1994.

[6] Sahama, L. Sim pson and B. Lane, " Security and Privacy in eHealth: Is it possible? ," IEEE 15th International Conference on e-Health Networking, Applications & Services (Healthcom), pp. 249-253, 2013.

[7] D. Liveri, A. Sarri and C. Skouloudi, "Security and Resilience in eHealth: Security Challenges and Risks," ENISA, 2015.

[8] JHS 179, "Enterprise architecture planning," 30 01 2018. [Online]. Available: http://www.jhssuositukset.fi/web/guest/jhs/recommendations/179.

[9] A. Hummelholm, Cyber Security and Energy Efficiency in the Infra structures of Smart Societies, Jyväskylä: University of J yväskylä, 2019.

[10] Dragon1-open EA Method / Visu alization Standard, "Enterprise Architecture Framework," [Online]. Available: http://wigi.dragon1.org.

[11] A. Hummelholm and K. Innala, "Intelligent Base Station Comprising Functions Relevant to its Operation,". US Patent 8,606,320 B2, 10 12 2013.

[12] A. Hummelholm, "Communications Network," Systems and Device, vol. 119900, 2009.

[13] A. Hummelholm, "E-health systems in digital environments," 18th European Conference on Cyber Warfare and Security, pp. 6 41-649, 2019.

[14] Eurostat, "Sustainable development in the European Union: Monitoring report on progress towards the SDGs in an EU C ontext," European Union, 2018.

[15] symbIoT, "symbIoTe project," 2018. [Online]. Available: https://www.symbiote-h2020.eu/.

[16] SHAPES project, "Grant Agreement ID: 857159," European Commission, 2019.

[17] International Alliance of Patients' Organisations, "Patient empowerment: for better quality, more sustainable health services globally," All Party Parliamentary Group, London, 2014.

[18] Lettieri, E. et al., " Empowering patients through eHealth: a case report of a pan-European project," BMC Health Serv Res, vol. 15, no. 309, 2015.

[19] M. Lehto and L. Martti, "Health information privacy of activity trackers," 16th European Conference on Cyber Warfare and Security, pp. 243-251, 2017.

[20] R. S. Laufer and M. W olfe, "Privacy as a concept and a social issue: A multidimensional developmental theory," Journal of social Issues, vol. 33, no. 3, pp. 22-42, 1977.

[21] T. Dinev and P. Hart, "An extended privacy calculus model for e-co mmerce transactions," Information Systems Research, vol. 17, no. 1, pp. 61-80, 2006.

[22] R. Pirinen, "Towards common info rmation sharing: Study of integration readiness levels," 7th International Joint Conference on Knowledge Discovery, Knowledge

Engineering and Knowledge Management, pp. 355-364, 2015.
[23] OpenNCP, "OpenNCP Installation," 2015. [Online]. Available: https://openncp.atlassian.net/wiki/display/ncp/OpenNCP+Installation.
[24] ECHO, "Health Care Sector," 20 19. [Online]. Available: https://www.youtube.com/watch?v=X9ViO1w_9ko.