The supply chain of a Living Lab: Modelling security, privacy, and vulnerability issues alongside with their impact and potential mitigation strategies

Kitty Kioskli[1,2,3*], Daniele Dellagiacoma[4], Theofanis Fotis[4] and Haralambos Mouratidis[1]

[1]University of Essex, School of Computer Science and Electronic Engineering, Institute of Analytics and Data Science (IADS), Essex, United Kingdom
[2]Gruppo Maggioli, Research and Development Lab, Athens, Greece
[3]trustilio B.V., Amsterdam, Netherlands
[4]University of Brighton, School of Sport & Health Sciences, Centre for Secure, Intelligent and Usable Systems (CSIUS), Brighton, United Kingdom

Received: November 25, 2021; Accepted: May 18, 2022; Published: June 30, 2022

Abstract

Worldwide, vulnerabilities and weak security strategies are exploited everyday by adversaries in healthcare organizations. Healthcare is targeted because these crimes are high-reward and low-risk. The attacks differ every time, from hacking medical devices, such as sensors, to stealing patients' data from electronic health records databases. The effects of these attacks are both short and long term lived, depending on the incidence handling process that each sector is adopting. The Covid-19 pandemic has exposed, in full, that healthcare systems are vulnerable and vastly unprotected while representing a threat to global public health. An important part of the healthcare ecosystem, for the development and validation of innovative tools and methodologies, is the Living Labs which are community-based and adopt co-creation as their primary approach. Because of the many stakeholders involved in the processes of the Living Labs, cybersecurity ought to be in their center. Besides the proven great importance of the Living Labs as part of healthcare, there is no research on security and privacy issues around them. The main purpose of this paper is to explore the supply chain of a Living Lab and identify its security and privacy challenges alongside with its vulnerabilities. The SecTro tool has been used to provide a thorough analysis which follows the Privacy-by-Design approach. The originality and novelty of our work are shown from: (i) moving one step further from desk studies by including requirements from citizens and professionals; (ii) being integrated into an effort from various researchers to supply a holistic approach to Data Privacy Governance; (iii) the first time which a paper is considering and analysing the supply chain of the Living Labs.

Keywords: Living Lab, digital health, supply chain, security, privacy, mitigation actions

1 Introduction

In this digital era, healthcare organizations have been a target for attackers because of the challenges and vulnerabilities they are facing. Breaches in privacy and security usually refer to cyberattacks, which is when a set of information is stolen, hacked, transferred, or corrupted by unauthorized individuals.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 13(2):147-182, June 2022
DOI: *10.22667/JOWUA.2022.06.30.147*

*Corresponding author: University of Essex, School of Computer Science and Electronic Engineering, Institute of Analytics and Data Science (IADS), Essex, United Kingdom, Email: kitty.kioskli@essex.ac.uk

Worldwide, vulnerabilities and weak security strategies are exploited everyday by adversaries in healthcare organizations [1]. The attacks differ every time from hacking medical devices, such as sensors, to stealing patients' data from electronic health records (EHR) databases. The effects of these attacks are both short and long term lived, depending on the incidence handling process that each sector is adopting. The Covid-19 pandemic has exposed in full that healthcare systems are vulnerable and vastly unprotected while representing a threat to global public health[2, 3].

Evidence from recent reports indicates that more than 90% of the healthcare infrastructures have experienced a cybersecurity breach [4], especially in the form of phishing emails which have increased by 473% in the last two years [5]. Healthcare, in particular, is targeted because these are high-reward and low-risk crimes. The attackers benefit greatly from the attacks both financially, as a complete set of medical information could be worth more than $1000, per affected person, [6], and politically, for example, by promoting cyberwar campaigns. The impact of these attacks is clearly seen on society and people [7].

An important part of the healthcare ecosystem, for the development and validation of innovative tools and methodologies, is the Living Lab approach. The Living Labs were first introduced in the early 2000s based on the initial concept by MIT in the 1960s, which proposed the transfer of research from laboratories to real-life settings [8, 9]. In 2014 the European Commission included the concept within the Innovation Europe Common Strategic Framework and since then a European network of Living Labs has been created, called the 'European Network of Living Labs' [10]. While there are definition divergences in the literature, ENoLL [10] has provided the following, widely adopted, definition: "The Living Labs are user-centred open innovation ecosystems based on a systematic user co-creation approach, integrating research and innovation processes in real-life communities and settings". More specifically, they are treated as a multidisciplinary approach, which considers societal problems, occurring in a physical or virtual space and involving several stakeholders (e.g., patients, healthcare professionals, manufacturers of medical devices) [11].

Because of the complexity of the infrastructure, the large variety of stakeholders, shared data, and the communication channels involved in a Living Lab ecosystem, cybersecurity ought to be in the center of the labs. Besides the proven great importance of the Living Labs as part of healthcare, there is no research on security and privacy issues around them and relevant analysis of their supply chain. This gap in the literature is aimed to be covered in this paper by the following set of objectives and research questions. The term supply chain includes a system of people, activities, organizations, resources, and information to produce a service or product [12]. In a Living Lab a supply chain includes actors (i.e., research staff), assets (i.e., sensitive data), policies (i.e., ethics), goals (i.e., health benefits), process activities (i.e., data management) and operations (i.e., surveys).

The primary objective of this paper is to identify and model privacy, security and vulnerability issues related to the Living Labs. The secondary objective is to raise the security awareness of the professionals and participants of a Living Lab and propose relevant mitigation strategies. More specifically, to address the set objectives the following set of research questions will be explored:

- What is considered the supply chain of a Living Lab?
- Which are the identified privacy and security issues of this supply chain?
- Which are the identified vulnerabilities of this supply chain?
- Which are potentially feasible and effective mitigation strategies that can be adopted?

The rest of the paper is organised as follows. Section 2 aims to provide a security overview in healthcare and move to a more particular part of the ecosystem, the Living Labs, in Section 3. Then,

Section 4 presents our security, privacy, and vulnerabilities analysis in the context of a Living Lab using a state-of-the-art methodology from the security and privacy engineering disciplines. Finally, in Section 5 we discuss the main findings of our study, limitations, and future research.

2 Privacy, security, incidence handling and risk management in healthcare

Even though the concepts of privacy and data protection, in general, have numerous similarities, these concepts differ. There is an overlap between them, but their differences shall be highlighted for the purpose of this paper. Further security challenges and vulnerabilities, specific to the healthcare concept, will be presented in this section. Lastly, incidence handling processes will be discussed.

2.1 Privacy and data protection

Data privacy represents a great challenge for organizations, particularly in fields where sensitive personal data of participants need to be handled. There is a number of practices and guidance documents (i.e., FDA, HIPAA), regulations (i.e., GDPR, Health Insurance Portability and Accountability Act,) and directives (i.e., NIST) which need to be followed in order to ensure privacy and data protection, however these do not overlap or communicate with each other.

An article entitled 'The Right to Privacy' was published in 1890 [13], which provided us with the first definition for privacy as 'the right to be left alone'. This definition was used extensively over the years, however, since then other definitions and various classifications have arisen providing more details on the concept of privacy. A recent and generally adopted classification, provided by Densmore [14], classifies privacy as follows: Information Privacy which is defined as a set of rules that controls the collection and further use of personal information; Bodily Privacy which is defined as a set of rules that safeguards the physical being; Territorial Privacy which is defined as a set of rules that safeguards the environment of a person and Communication Privacy which is defined as a set of rules that safeguards communication and means of correspondence.

The privacy typology is not set in stone, there have been many definitions and adaptations. This somewhat fluid and open to interpretation concept creates barriers for the experts and individuals who need to follow it. Despite the differences in the classifications of privacy, the concept of personal data is found in the center of information privacy. However, this claim shall be treated with caution, as personal information can be processed in activities that interfere with other privacy classes. That means that information privacy does not pervade all other classes of privacy. However, information privacy does not occur simultaneously with the full scope and meanings of other privacy classes. Therefore, privacy is older, especially if we take into consideration the historical efforts to define and regulate it, and a broader concept than personal data. It might also be indicated that privacy incorporates the concept of personal data and has been used as the basis to develop personal data protection.

In any information system, including healthcare organizations, the milestones that should be taken into consideration are privacy and confidentiality. Privacy by design (PbD) is a very important process including good private practices in the operation and design of information technology (IT) systems, business practices and physical infrastructures [15, 16]. PbD aims at securing privacy and obtaining control over personal information to get a competitive and sustainable advantage on top of organizations [17]. Healthcare infrastructures are benefiting greatly from PbD and it is essential as privacy is being considered from the initial designing stages, however, this shall be applied in a wider fashion.

2.2 Healthcare security, challenges, and vulnerabilities

The healthcare ecosystem is repeatedly affected by cybersecurity attacks while breaching the privacy and disrupting the data protection of the organizations and the individuals. These security incidents may result in short- and long-term effects from the unintentional or intentional release of personal identifiable information to the disruption of the clinical care [7]. Ponemon Institute has recently stated that "healthcare organizations are in the cross hairs of cyber attackers" and this only worsens over time. In US healthcare facilities it is estimated that one cyberattack takes place every month and most of them have lost or exposed patients' personal information [18].

To continue with, a recent report by the European Union Agency for Cybersecurity (ENISA) [19] revealed that compared to other sectors, the healthcare infrastructure is critical and one of the most vulnerable. This can be explained by the great value of the assets within healthcare organizations and by how easily they can be attacked by adversaries. Medical personal data can be valued up to 20 times higher than, for example, financial data. This is because the data derived from healthcare records can be continuously used and exploited, even if the security breach which released them has been resolved. Meanwhile, healthcare organizations are lacking behind other industries, such as insurance or pharmaceutical companies, in safeguarding their data and infrastructures.

Considering the aforementioned information, the IT security in the healthcare industry, applications and services are of paramount importance and major concern. This is explained by the confidentiality and privacy issues around sensitive healthcare data. There are various security challenges, which differ according to the relevant sectors as well. Some overlapping challenges found in the literature are the following, as presented in Table 1.

Apart from the security challenges, the changes, and the use of new technologies result into the exploitation of software, hardware, and human-centric vulnerabilities by adversaries. Some of these changes which contribute into the exploitation in healthcare infrastructures are: the increased use of Internet of Medical Things (IoMTs), such as sensors, and the use of remote networks and systems for their maintenance; the use of personal equipment, such as laptops, mobile phones, by the hospital personnel and the patients which may not be up to date with security standards; the struggle of the IT personnel to supply certified security solutions due to the numerous and overlapping security standards and inadequacy of training in the staff; and the necessary processes which have to be followed to monitor patients' intake and discharge within hospitals. Potential attackers with strong skills in the cybersecurity field take advantage of the identified vulnerabilities and perform cyberattacks in the networks, systems and IoMTs.

2.3 Incidence handling in healthcare

Incidence handling is vital when it comes to security, privacy, and vulnerability issues. In this sub-section we will present two widely applicable and adopted incidence handling processes, aiming to provide some information on how healthcare organizations tackle upcoming security incidents. Based on ENISAS's report [19], incidence handling represents one of the main challenges in the security of the healthcare ecosystem. Although there are security policies in place to protect the healthcare infrastructures, cyberattacks take place which cannot be avoided or anticipated. These security incidents have roots in malicious actions (e.g., human interventions aiming for the disruption of workflow), natural disasters (e.g., fire or flood in the building where the servers are located), human errors (e.g., negligence or oversights) and system failures (e.g., insufficient computer memory). It is worth noting that most security breaches occur due to human errors or system failures.

Therefore, healthcare infrastructures ought to have an incidence response capacity to accurately and timely identify security incidents and further restore the systems in the safest way. The National Institute of Standards and Technology (NIST) [20] has introduced a guide including four phases for the cyber-

incident handling process as presented in Figure 1. This guide is adaptable, flexible and can be utilized by healthcare organizations.

All four phases are of equal importance and are interconnected. In order to give more details on this cyber-incidence handling process an in-depth analysis of the major phases is presented in Table 2.

Moving forward, ENISA [19] suggests that one of the most efficient ways to tackle cybersecurity threats is the creation of a global ecosystem of computer security incident response teams (CSIRTs) and security operations centers (SOCs). CSIRTs and SOCs should be able to share information, communicate and respond to cyberthreats. CSIRT involves a set of services such as security monitoring, information and cybersecurity incident handling, vulnerability management, cybersecurity knowledge management and situational awareness. The five different phases are presented in Figure 2. A SOC involves an incident detection service that occurs via observing technical events in systems and networks while they may also be accountable for incident handling and response. This applies to healthcare organizations as well, as an effective method to respond to cyberattacks.

Table 1: Security Challenges in Healthcare.

Challenge	**Description**
Systems Availability	Concerning continuous accessibility of critical health information by authorized professionals to ensure the best healthcare services. Systems availability may correlate to physical systems function (e.g., storage, networks) and may significantly affect the delivery of healthcare.
Confidentiality	In regard to sensitive personal data which require urgently to follow privacy and security standards/directives/laws.
Access Control & Authentication	Authentication is the first stage of the user's validation to confirm their identity. This is necessary to ensure that the users are authorized to access the system, which is a key-security feature in healthcare organizations.
Data Integrity	It aims to ensure the integrity and quality of the data that are exchanged and stored for administrative and clinical purposes. This is a very important part of healthcare systems since errors in health or personal data may directly affect an individual's medical treatment or insurance claims.
Network Security	This is fundamental to secure healthcare organizations, particularly when the systems are network-based (e.g., cross border eHealth, EHRs).
Security Expertise & Awareness	This is critical and includes the sufficient and adequate organizational structure in addition to the role of a security or data protection officer.
Data Loss	It is considered essential to not lose data since they can easily and quickly become compromised. This is important as confidential, personal, and health data are stored digitally.
Incident Handling	Typical security incident handling includes the incident response and management. This is the protection of an organization's information by developing and implementing incident response processes (e.g., management oversight), to quickly identify the attack, then effectively minimize the damage, eliminate the attacker's presence, and successfully restore the integrity of the systems and network.

In particular, the five phases of CSIRT's lifecycle can be depicted as follows:

- Assessment for Readiness: The first steps of the establishment of a new CSIRT, that includes a discussion regarding the reasons and necessity for creating a CSIRT, an estimation for the budget and creating requirements for the next phase.
- Design: This phase creates detailed plans for the next step that should be taken, and its requirements are all the outcomes from the assessment to the readiness phase.
- Implementation: This phase covers organizational matters such as technology, governance, people, services, and processes.
- Operations: During this phase the CSIRT which has been created delivers the CSIRT services.
- Improvement: It is the phase that a CSIRT creates requests for improvements, prioritizes initiatives and receives a budget for the 'design-implementation-operation-improvement' cycle.

Both the cyber-incidence handling process by NIST and the lifecycle of a CSIRT and SOC by ENISA are vital methods for incidence-handling and are adopted widely in industries in general while, on occasions, they are adopted in healthcare as well. Indeed, there is an urgent and pressing need for the development and evaluation of incident handling reporting classification specifically dedicated to the needs of the healthcare sector at a pan European level. Good practices from the international landscape shall be considered to move in this direction.

3 The Living Labs

This section will give an overview of the structure of the Living Labs and their supply chain. Following that, attack scenarios and the vulnerable groups of this supply chain will be further discussed, as well as user requirements as identified in an EU funded project. Lastly, mitigation strategies in relation to the user requirements, attack scenarios and identified vulnerable groups will be introduced.

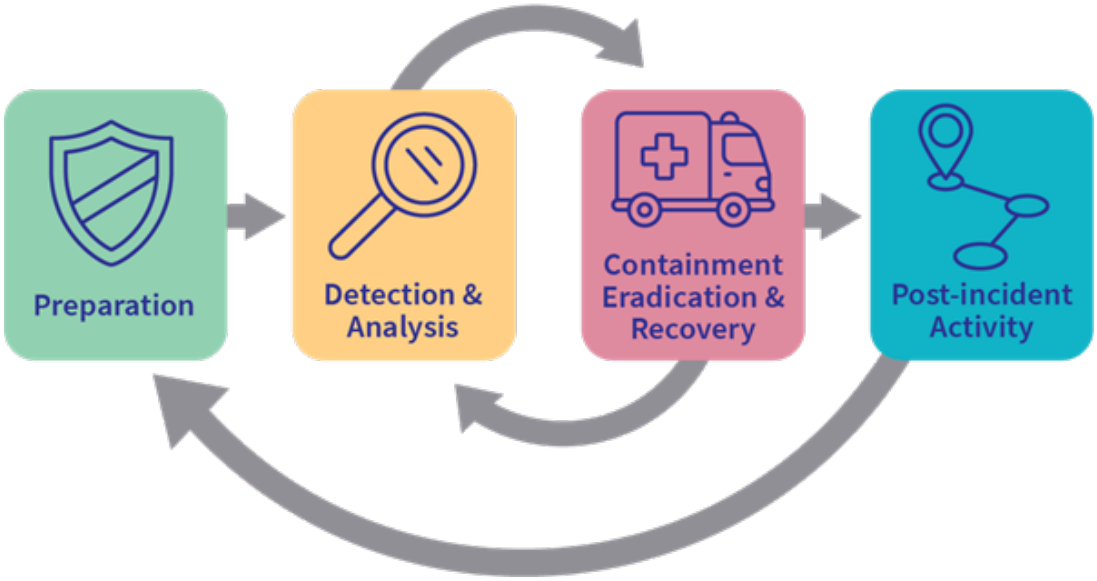

Figure 1: Cyber-Incident response cycle [20].

Table 2: Analysis of the Cyber-Incident Handling process.

Phase	Analysis
Preparation	It involves the steps that are taken before a security incident occurs (e.g., crossover cables). Preparation contains potential incidents that may be required to be managed or ways to make incident response more efficient.
Detection & Analysis	This phase involves the detection of incidents and the analysis of these incidents, to explore the possibility that they represent a security incident. If they represent a security threat, the threat level (e.g., high, medium, low) is further explored.
Containment, Eradication & Recovery	This containment phase is when the incident response team attempts to minimize the damage from an incident (e.g., isolating traffic, powering). The eradication phase contains the process of understanding the cause of the incident. The recovery phase includes the cautious restoration of the systems to be operational.
Post-Incident Activity	This phase includes the composition of a follow-up report. Each incident response team should grow to identify new threats, improve technology, and lessons learned aiming to reduce the probability of a similar incident re-occurring and to improve the incident handling process.

Figure 2: The CSIRT's Lifecycle.

3.1 The supply chain of the Living Labs

A digital health Living Lab is an open innovation user-centred ecosystem. The Living Labs are based on systematic co-creation and co-production while integrating research and innovation processes in real-world settings [21]. The UK Department of Health Personalisation Communications Toolkit defines co-production as, groups of people who come together to affect the way particular services are designed, integrated, and delivered or when individuals are able to affect the services they receive. Living Labs are used as tools for the integration of research and innovation processes, where various stakeholders receive tailored services according to their needs. The main stakeholders involved in a Living Lab are

presented in Figure 3. It is worth exploring in detail the supply chain of a Living Lab in order to be able to accurately identify its security challenges, privacy issues and vulnerabilities, as discussed in the analysis performed in Section 4.

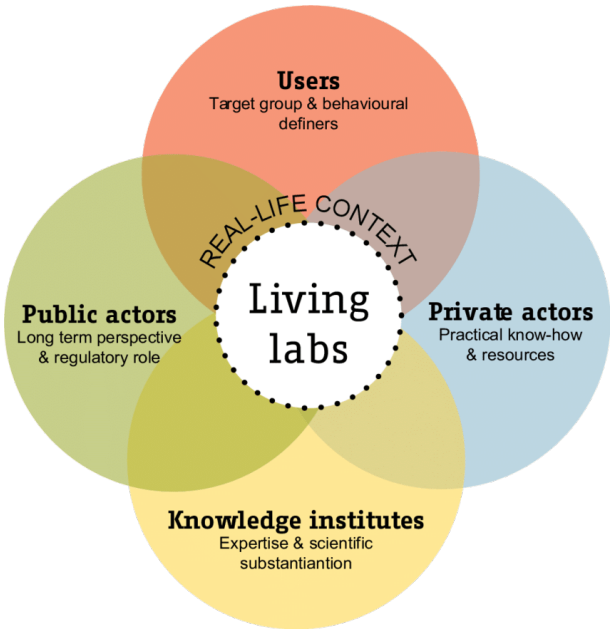

Figure 3: Stakeholders involved in a Living Lab [21].

The detailed supply chain, of the main stakeholders involved in a Living Lab, is the following:

Citizen/Patient: The users are typically local residents which come together to factor in health innovation, by providing input from their own experiences and perspective. Each resident has the unique opportunity to help other residents and/or collaborate with them to influence health innovation, which could become applicable worldwide. Users have access to cutting edge technology services, before they reach the market, they get informed first-hand and affect the final version of the services which will be provided to the general population.

Public Actors: Public actors, as for example local councils, utilize the Living Labs for inspiration development and evaluation of new services or regulations. They aim in creating sustainable welfare solutions which would be applied to the general population and benefit from them. The public actors contribute their staff to engage with end users involved in the Living Labs and develop or test new approaches and services. At the end of the process, the staff become more knowledgeable and aware of the users' needs, while they are capable to deliver healthcare and welfare services with embedded technology or regulate areas in healthcare as needed.

Private Actors: Private actors, as for example digital health technology developers/engineers, site managers and start-up companies, also get involved in the Living Labs and are a vital element in this ecosystem. They are interested in feedback on their products in the product's whole lifecycle from the conceptualization, production or prototype phase to the final testing and evaluation. The private actors collaborate with the residents as end users, seeking their input on user design and feedback on the product they are interested to research at the time.

Knowledge Institutions: Another important component within the Living Labs are knowledge institutions, as for example academia via universities and research centres. In this instance the Living Labs are utilised for training and research purposes. Training purposes include potential clinical placements or internships for undergraduate or graduate projects. While research purposes include field work

for research projects via recruitment and data collection through quantitative and qualitative methodologies. Academic institutions have a vital role also of safeguarding the participants ensuring ethical and responsible conduct of research and collaboration between the stakeholders.

The supply chain is interconnected and constantly interactive, making sure that the input comes from the relevant actors and applied accordingly. Community and domestically household based Living Labs are presented with IoT proliferation, integration of sensors, low powered wireless communications, and traditional home broadband WiFi and internet services. As such, they become ecosystems of information technology connectivity. Though, these technologies are designed for specialist environments (i.e., controlled medical data collection), in a Living lab ecosystem they converge within a general consumer landscape. The Living Labs become the testbeds for the co-production of digital health solutions, through ubiquitous access to rich and interactive technology. However, the supply chain also inherits the emerging risks and vulnerabilities that come with the testing and use of these technologies [22, 23]. Hence, the extreme diversity between devices, sensors, third party applications and the variety of stakeholders, means that a Living Lab is particularly vulnerable to supply chain malicious attacks which can be performed by attackers. Potential security attack scenarios are identified and presented in the upcoming section.

3.2 Security attack scenarios and vulnerable groups in a Living Lab

Because of the nature of a Living Lab, as an open ecosystem, establishing cybersecurity practices can be challenging and attacks may easily be pursuit by adversaries. There is constant data exchange via various communication channels between stakeholders, such as citizens, local councils, researchers, and technology companies. Because of the interaction of multiple groups of people, it is unavoidable that they have different levels of security and privacy awareness and knowledge as well as different ways to use hardware and software systems. Consequently, this diversity and complexity raise the risk at higher levels.

Potential attacks may target any stakeholder and phase where information is exchanged. Hence, potential general attack scenarios include eavesdropping, phishing, and malware. Since a Living Lab is used as a test bed for healthcare technological devices by users, an attack can be performed irrespective of the device. For the purposes of this paper specific attack scenarios have been identified and explained below in Table 3. These scenarios derive from a recent European funded project, entitled 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) [24] aims to develop a solution that improves the detection and analysis of cyberattacks and threats on healthcare information infrastructures (HCIIs).

The most vulnerable groups regarding cybersecurity incidents, in a Living Lab, are found to be citizens/patients, followed by researchers and healthcare professionals [24]. More specifically, citizens/-patients are the most vulnerable group as the consequences rising from a cybersecurity incident, would affect them the most. Though, the full extent of the impact is not possible to be estimated, it can only be hypothesised that it could even have a detrimental impact on the health and wellbeing of these users. Following that, the second most vulnerable group in a Living Lab, which are the researchers and healthcare professionals, may also experience a great impact due to a cybersecurity breach. This is because their work involves the collection of sensitive data that supports important decision making, and they might have low cybersecurity awareness to prevent or act on such incidents. Hence, they are considered relevant gateway for cyberattacks and malware. Hospital managers and hospital staff in general are also at a medium to high risk for attacks. As we have seen in recent events, such as in the UK and Ireland, the attackers target the hospital as a whole organization by gaining control of their systems and ask for excessive amounts to be paid in ransom for the hospital to regain control.

Table 3: Potential attack scenarios and impact in a Living Lab.

Description	Scenario	Impact
Attack on a telehealth device	An adversary steals the telehealth device, gains direct access to the hardware, and exploits user credentials.	The adversary could easily access data in the manufacturer's platform.
Direct attack on the wireless infrastructure in the Living Lab	The adversary by exploiting a vulnerability, gains access to the wireless network stack.	The adversary could access the data on the personal devices of the users.
Indirect attack between the telehealth device and a smartphone	The adversary conducts a man in the middle attack between the device and the app on a smartphone.	The adversary collects and alters all transmitted data.
Attack on the software operating on the telehealth device	The adversary attacks the software operating system to gain control over it.	The adversary access all collected and transmitted data and gains access to the cloud.
Deletion of all or selected data	The adversary deletes database tables or other resources in server.	Disruption of the services by the users.
Data encryption	The adversary encrypts sensitive data to obstruct legitimate access.	The adversary asks for ransom and the users experience disruption of services.
Service attack	The adversary overloads the company's system with strong hacking skills. prohibit normal usage of the system.	The normal usage of the system and the quality of the users' healthcare are affected.
Social engineering	An adversary via social engineering convinces the authorised owner of the device to share important information.	The adversary gains access to personal information of residents stored on the manufacturer's platform.
Modification	The adversary after gaining system access modifies the data on the company's server to prepare for more attacks.	Information provided to users is incorrect leading to affected health.

3.3 User requirements in a Living Lab

As we have seen above, the combination and convergence of heterogeneous technologies being tested in a Digital Health Living Lab, with the lack of specialised security knowledge of the participating stakeholders, are the key challenges exacerbating the cyber threat to Living Lab ecosystems.

Our aim is to identify exactly these challenges as found in AI4HEALTHSEC) [24] since the project identified a complete list of user requirements (see Appendix A). To understand which user requirements, and why, apply to a Living Lab environment one must reflect on the impact a cyberattack might have on the stakeholders involved. A consequence of technology convergence in a Living Lab is the cascading effect of a compromise of one system to others. Conventional security breaches in cyberspace typically

result in financial loss, breaches of data privacy or loss of control of computer devices. Though Living Lab environments are typically set up for testing and trialling digital health technologies rather than providing health care services, the overall process can be disrupted by a cybersecurity breach, compromise or disrupt the devices and systems under testing, and the consequences can extend to exploitation of physical privacy, safety, and well-being of the end-users [23].

The user requirements directly relevant to a Living Lab are those that can address collectively the requirements of participating stakeholders within the complexity of the ecosystem/infrastructure and have been divided into the following categories (see Appendix B):

- Threat prevention: This includes requirements related to risk assessment and management. Typically, threat prevention relies on a robust understanding of the cyber security needs, risk appetite, and risk tolerance for the key digital health devices and ICT infrastructure of the Living Lab.
- Threat detection: This is a proactive control measure in defending the supply chain against potential attacks. The methodology shall automatically detect a potential cyberattack and adversary's actions using autonomous intelligence swarm agents and reporting to the supervisor agents.
- Threat awareness: This includes alignment with the incident response and post-incident activities to ensure mitigation of the threats and risks and overall business continuity. Furthermore, it relates to enhancing and updating the threat intelligence information and incident response planning, through lessons learned from the evolving threats, risks, and related incidents.

It becomes apparent that from a number of proposed 67 requirements, only 16 can be perceived as non-directly related to the ecosystem of a Living Lab. Mainly, these are the functions that could provide real-time decision-making support for incident response, post-incident review activities, and relevant metrics covering reliability, credibility, acceptance, timeliness, and realism of risk management goals. Two are the reasons for excluding these requirements: Firstly, the fact that the tested technologies are not connected with wider healthcare infrastructures but rather limited to the ecosystem's connected networks, meaning that a potential attack will not affect sensitive data. Secondly, is the limited specialised security knowledge of the involved stakeholders where this information would not make much sense and be of much use. The identification of the user requirements relevant to the Living Labs has been proven uniquely useful as it provided input for the next Section of this paper, including our main analysis, and modelling of a Living Lab ecosystem.

4 Modelling the ecosystem of a Living Lab

This section provides the results of our main analysis regarding the security challenges and vulnerabilities in the supply chain of a Living Lab. The analysis aims to be generic enough to cover all Living Labs rather than a specific establishment. The main tool used for this analysis is SecTro. SecTro helps the security/privacy analyst to model different areas of an organisation from collected information and further improves the organization's GDPR compliance.

4.1 Method

To model the ecosystem of a Living Lab, we used the SecTro tool. SecTro is a Computer-Aided Software Engineering (CASE) tool which has been chosen because it is flexible and supports the analysis of an infrastructure from different perspectives. It differs from other tools because it provides the analyst with automatically generated models based on data collected and can further feed other tools at an implementation/technical level. This tool guides and supports the analysts in the construction of appropriate

models, implementing the Privacy by Design (PbD) approach. The PbD approach is based on the Secure Tropos methodology [25, 26, 27, 28, 29, 30, 31, 32]. Secure Tropos follows the principles of the Goal Oriented Requirements Engineering (GORE), using goals to represent the intentions of the stakeholders. One of the main advantages of Secure Tropos is its requirements-driven approach to support the analysis from the early stages. Furthermore, the methodology includes social concepts such as goals and actors to promote a socio-technical analysis focused on privacy. Secure Tropos supports both analysis and design thanks to implementations of multiple models representing different abstraction levels, also called views.

Even though Secure Tropos has been selected as the basis for the approach implemented by the SecTro tool, the methodology has been extended with concepts and relations inspired by PbD and GDPR as part of the DEFeND EU Project [33, 34, 35, 36, 37]. Some of the concepts introduced are: Privacy/Security Constraint, Data Asset, Third Party, Data Processing Activity, and relations between concepts such as "Performs" and "Validates". Moreover, new views related to PbD and GDPR have been introduced to allow the creation of specific models.

This approach is supported by the SecTro tool, which allows developers to create and analyse models based on the methodology. The SecTro tool has been developed through Eclipse Sirius, a technology that allows the creation of graphical models using the Eclipse resources. SecTro takes advantage of the different characteristics of Sirius. One of these features concerns the definition of rules that can be used to validate the models to verify the correct use of the language based on the metamodel. The tool offers a graphical user interface (GUI) to model the different views. The GUI provides a palette containing the concepts that can be used in the modelling area. Moreover, the elements can be moved around the modelling workspace and connected with each other to specify the relations. It is also possible to specify additional properties of a concept. The tool supports the analysis through different models, also called views. For this case study, we focus on three views: Organisational Structure, Data Mapping and Privacy-by-Design. It is important to note that in order to limit our analysis in the context of our paper we have set some boundaries in the supply chain of the Living Lab, and these are to restrict the information around privacy and security related components.

4.2 Organisational view

The first view represented by using the SecTro tool is the Organisational View. See Figures 4-5. The purpose of this view is to represent the organisational structure of the Living Lab ecosystem with all its main actors. Moreover, this view includes different elements such as processing activities, goals, purposes, assets, and policies associated with the different actors.

The first element to be modelled in this view is the Organisation where multiple actors engage in different activities. An actor is an entity that performs actions to achieve goals inside an organisation. A goal is a state to be achieved by an actor and it is often related to a processing activity which is an action upon personal data. To achieve a goal an actor can put into practice an operation that is the actual action performed by an actor. Finally, an asset is a resource of a different type (i.e., data, physical, software) used by an actor to execute an operation. In this case, the scenario represented is the implementation and the improvement of the IoMT devices to provide health benefits to citizens and patients within the Living Lab ecosystem.

In this scenario, we identified three main organisations involved. The organisations modelled for the Living Lab are the Local Council, the Private Company in charge of the technology implementation and the Academia that is responsible for the research activities. Each organisation includes different actors who operate within the departments. For instance, the Private Company includes the Engineers and the Site Managers. Instead, the actors involved in the Local Council are the Citizens/Patients and the Counsellors. Finally, the Research Staff is part of the Academia. Then, each actor can be characterised by different elements. For instance, the Research Staff can analyse the collected data. This processing

activity is directly connected to the Research Staff which is conducting research activities. To achieve its goal the Research Staff can use different methods. For instance, these operations are A/B testing, online surveys/interviews and focus groups, and randomized control trials (RCTs). To carry on with the interviews, focus groups and RCTs the Research Staff needs consent forms represented by SecTro as an asset. Moreover, another asset modelled is the Sensitive Data of the user collected during the interviews. Finally, SecTro can also model the policy that the organisation must be compliant with. For instance, the Research Staff needs to follow the GDPR rules collecting data from the surveys/interviews and respect the Ethical Approval for research activities. On the other hand, the Engineer from the Private Company can collect various data. This processing activity is performed to achieve the main goals of the Engineer which are to measure and improve user experience and improve IoMT devices. The Engineer uses online surveys/interviews and focus groups to improve user experience whereas A/B testing can help to improve the IoMT devices. Also, the IoMT devices are modelled by SecTro as a physical asset. Another actor, the Site Manager, also belongs to the same organisation as the Engineer. Instead, the Site Manager oversees the data management to achieve the Technology Implementation. In fact, the Newly Designed Hardware is tested through Feasibility trials and RCTs.

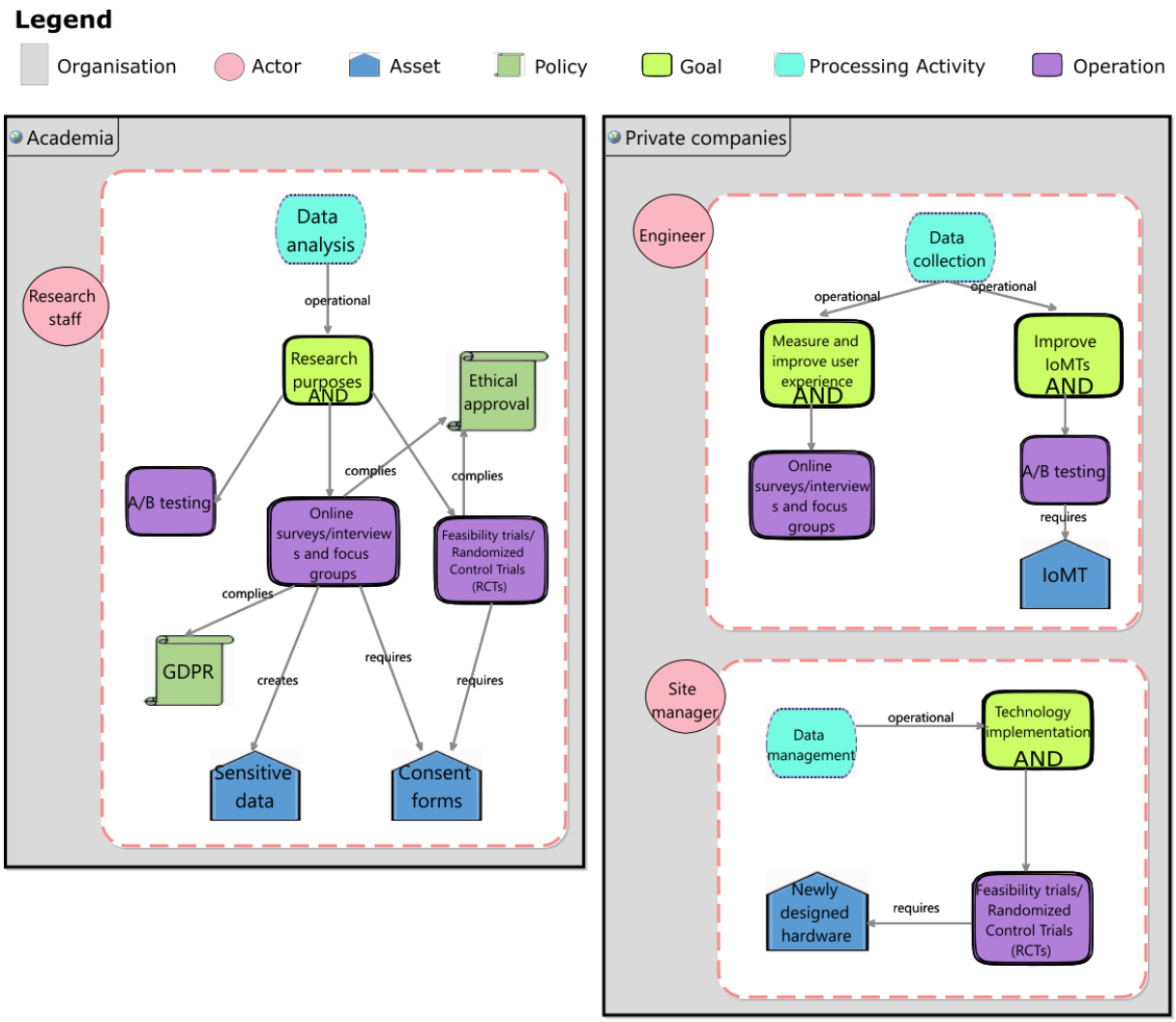

Figure 4: Organisation View regarding academia and private companies of a Living Lab.

The two remaining actors, the Citizen/Patient and the Counsellor are part of the Local Council. The Counsellor can store the Data focusing on Health Economics. To do that the Counsellor can update the EHRs with the information collected from the Citizens/Patients through surveys/interviews and focus groups. This operation regarding the collection and storage of Citizens/Patients' data needs to comply with Health and Safety Policies and the Declaration of Helsinki.

Finally, the Citizens/Patients exchange personal data with the other actors of the Privacy Lab. The exchange of this data aims at achieving the main goals of this actor which are Health benefits and Technology Acceptance. Data is collected in different ways including A/B testing, RCT and surveys. Usually, the A/B testing is carried on through the personal devices of the Citizen/Patient.

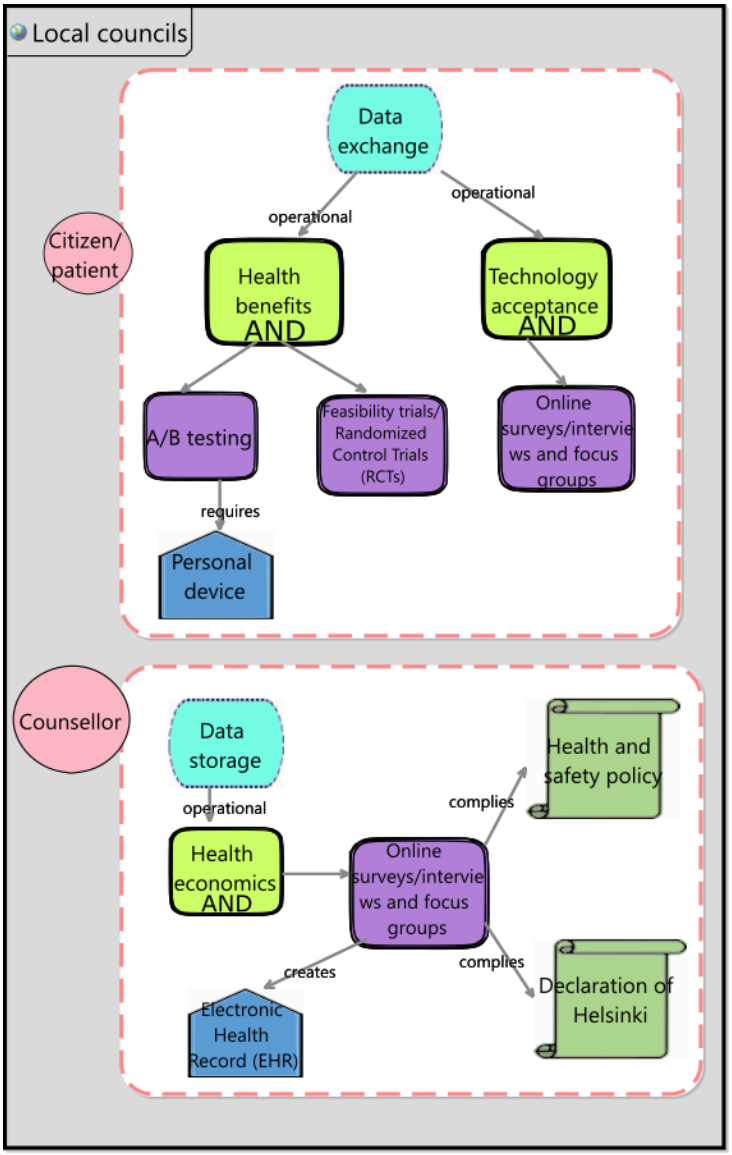

Figure 5: Organisation View regarding citizen/patient and counsellor of a Living Lab.

4.3 Data mapping view

After completing the Organisational view, we continue the analysis of the Living Lab ecosystem with the Data Mapping view depicted in Figures 6-7. This view already includes some elements from the previous analysis performed in the Organisational view. Specifically, the elements synchronised from the Organisational view are actors, goals, operations, and assets. In this case, all the actors such as the Research Staff, Counsellor, Citizen/Patient Engineer and Site Manager from the different organisations of the Living Lab ecosystem. Each of these actors includes their goals, operation, and assets from the Organisational view, and all the connections between them. Instead, the new element introduced in this view is the Data Action, which represents activity performed on an asset.

For instance, the different operations carried on by the Research Staff are connected to the management of the data collected. Indeed, the Research Staff uses sensitive data collected for research purposes. In a similar way, the Data Action performed by the Counsellor is the quantitative analysis of the EHRs. On the other hand, the Site Manager wants to perform a qualitative analysis of the data collected through the newly designed hardware. Finally, the Engineer collects data from the IoMTs to achieve his/her goals, measure user experience and improve the IoMTs.

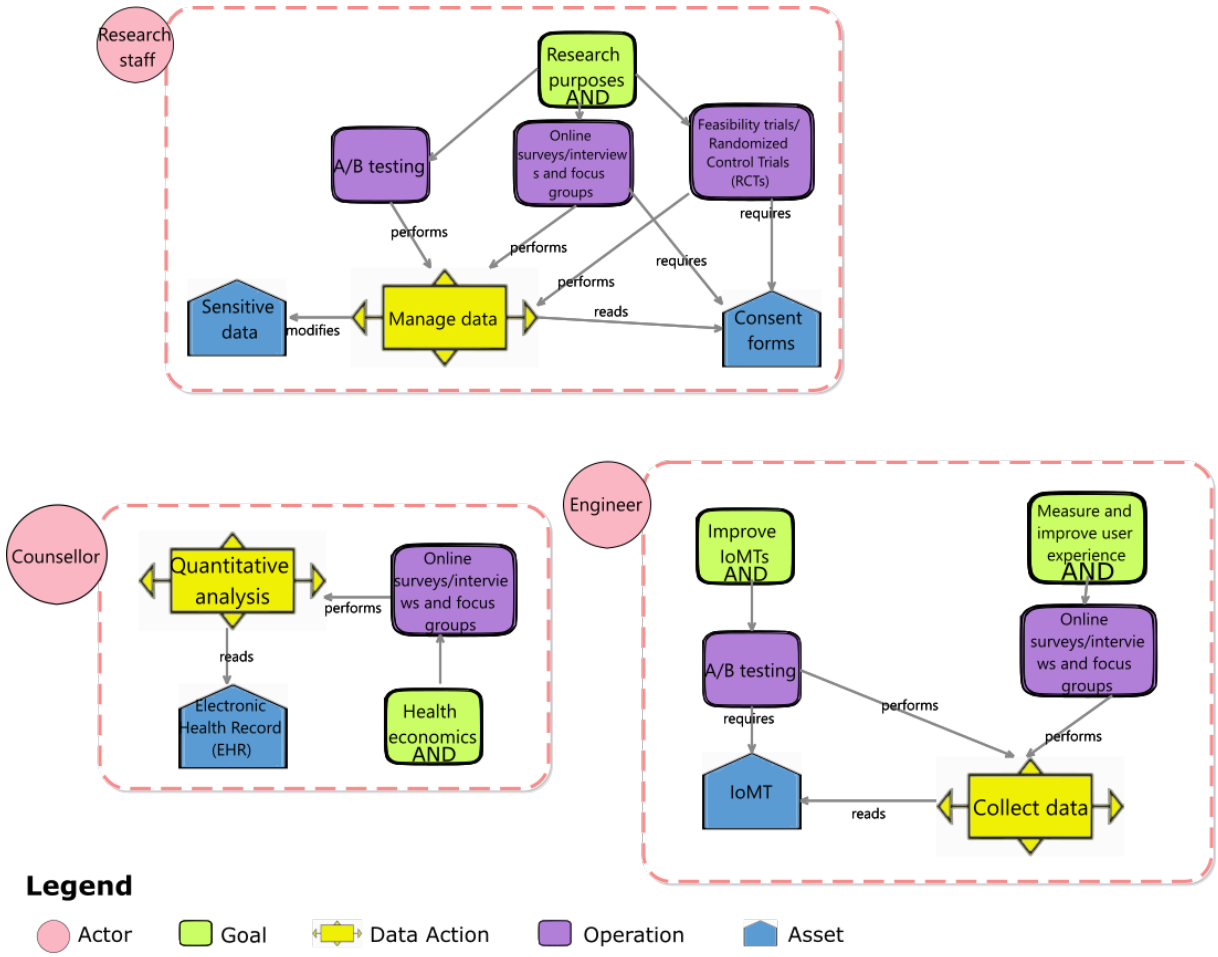

Figure 6: Data Mapping View regarding research staff and counsellor of a Living Lab.

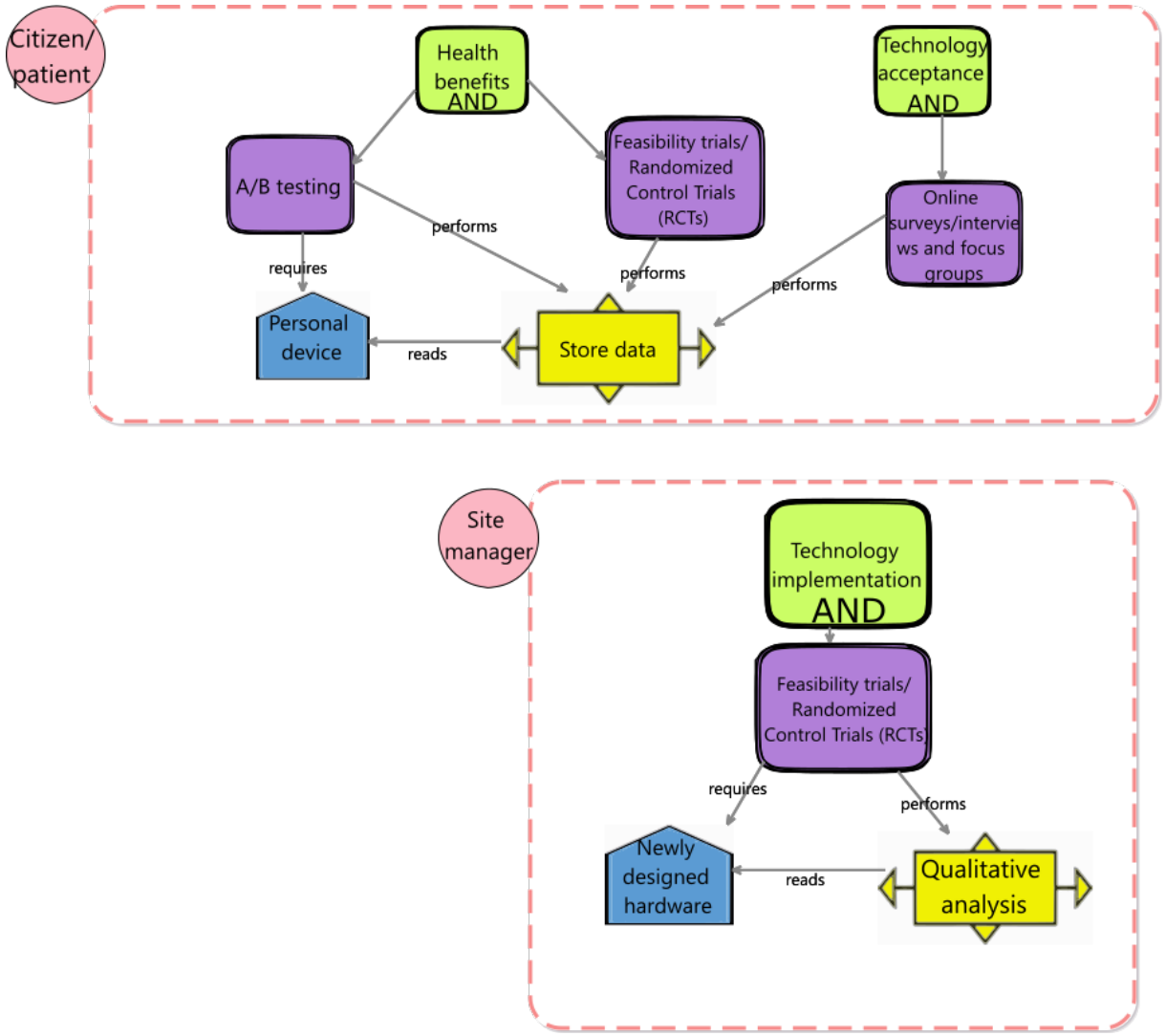

Figure 7: Data Mapping View regarding citizen/patient and site manager of a Living Lab.

4.4 Privacy by design (PbD) view

The PbD view already includes some elements identified in Organisational and Data Mapping views. In particular, we have all the actors with their operations and assets modelled in the other views. Instead, the PbD view includes new elements such as threats, constraints, mechanisms, and measures. These elements can be used during the modelling with SecTro to perform a comprehensive PbD analysis of the Living Lab ecosystem, as shown in Figures 8-9. In detail, threats are malicious actions that can have an impact on the assets of an organisation. Measures are high-level methods for satisfying privacy and security requirements whereas mechanisms are actual procedures to make a measure operational. Finally, constraints are privacy and security requirements related to an asset. The PbD view allows the analyst to model the potential threats that could impact the assets, in relation to their privacy and security constraints. Then, different measures can be used to satisfy those constraints and the actual mechanisms to protect the assets mitigating potential threats. For the Living Lab ecosystem, several potential threats have been identified.

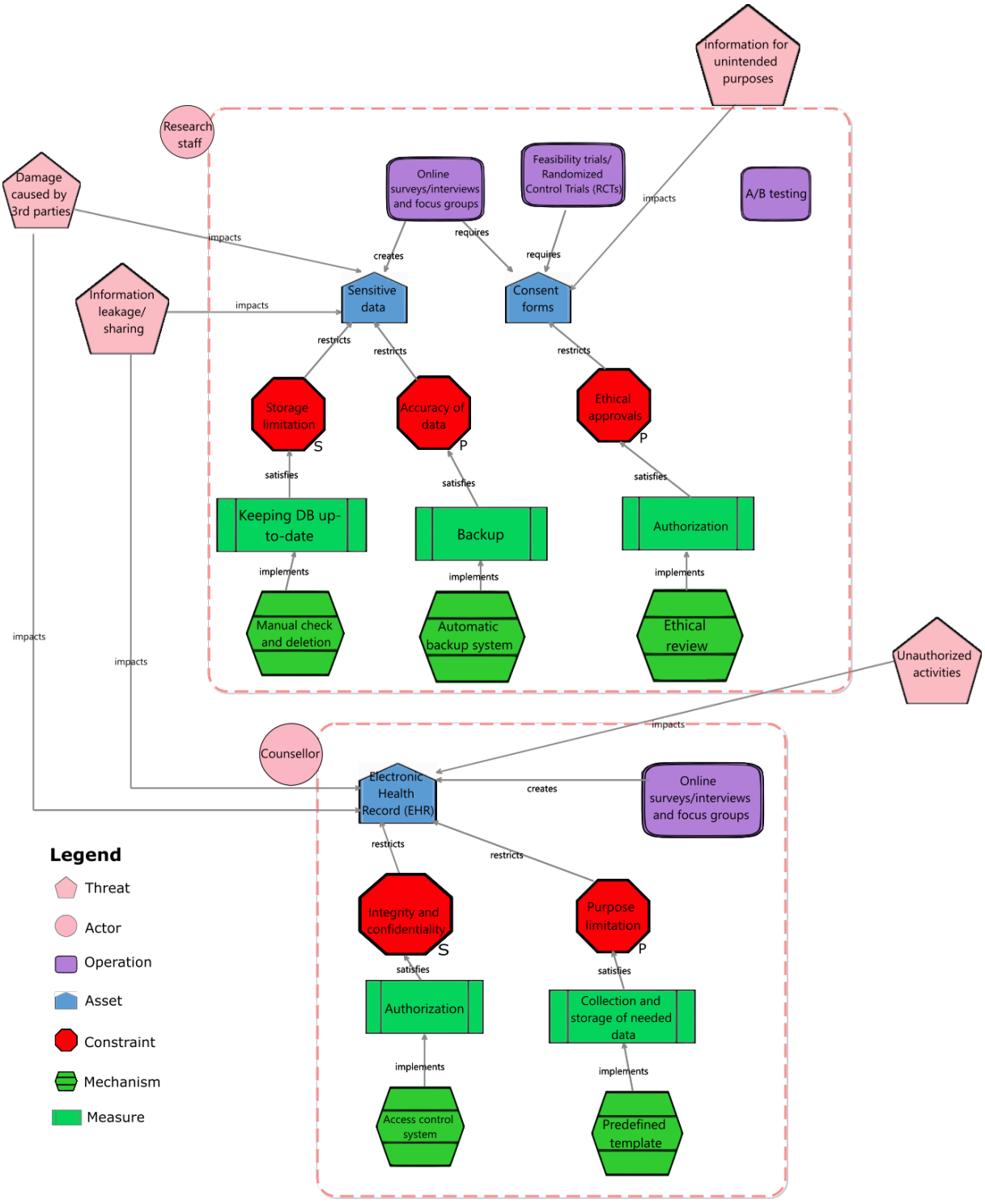

Figure 8: Privacy-by-Design View regarding research staff and counsellor of a Living Lab.

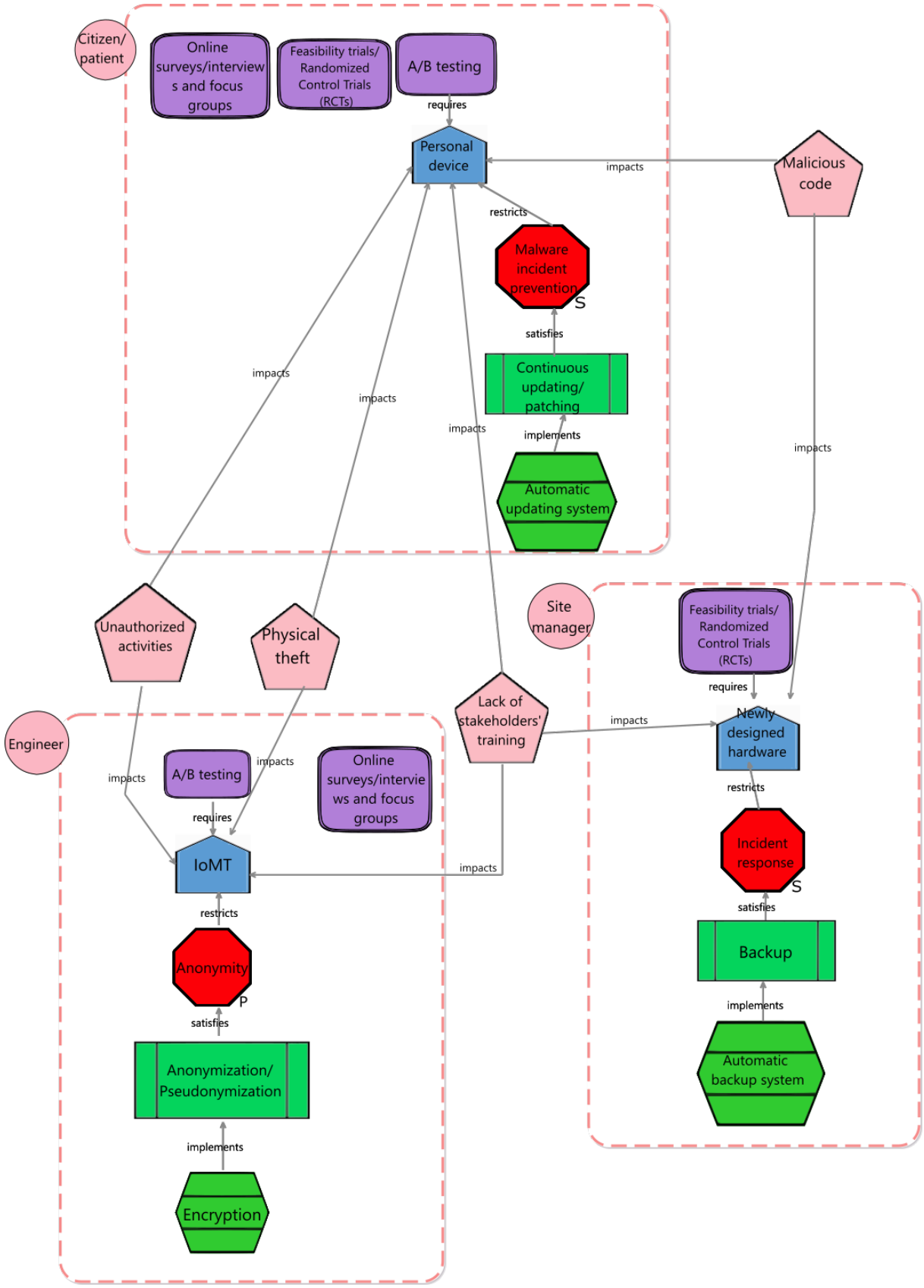

Figure 9: Privacy-by-Design View regarding citizen/patient, engineer, and site manager of a Living Lab.

The first one is the potential damage caused by third parties. This threat, as well as the other one called information leakage/sharing, can impact the sensitive data collected by the research staff and the EHRs managed by the counsellor. However, these two assets have different privacy and security constraints. For instance, the sensitive data collected by the Research staff are restricted by the storage limitation and the accuracy of the data. Keeping the database up to date through manual checking and deletion of data can be used to satisfy the storage limitation requirement. Instead, the Mechanism chosen to satisfy the accuracy of data is an automatic backup system. Another threat for the Research Staff is the Use of Information for Unintended Purposes. Instead, this threat could impact a different asset, the consent form. In this case, the privacy constraint for the consent form is the ethical approval. The high-level measure used to satisfy the constraint is the authorization of the consent form whereas the actual mechanism is an ethical review process.

Besides the threats described above, the EHRs could be affected by another threat named Unauthorized activities. Moreover, this threat can affect other assets such as the IoMTs and Personal Devices. The actor responsible for the IoMTs is the Engineer, and it must respect the privacy constraint that restricts the asset. In this case, the privacy constraint requires the anonymity of data collected from the IoMTs devices. For this reason, the anonymisation/pseudonymisation measure needs to satisfy this privacy constraint, and a mechanism such as encryption can be used to implement that measure.

Furthermore, personal devices of the citizens/patients along with the newly design hardware of the site manager can be threatened by malicious code. In order to ensure the security constraint, i.e., malware incident prevention, associated with the personal devices, continuous updating/patching is needed to fix vulnerabilities that could be exploited by malicious code attacks. For this reason, an automatic updating system can be used as a mechanism to mitigate the threat.

On the other hand, the newly designed hardware needs to satisfy the security constraint which guarantees a response in case of an incident. This can be achieved through an automatic backup system. Finally, two other threats can impact multiple assets. One of these is the physical theft of an asset. This could happen to the citizens/patients and the engineer who interact with personal and IoMT devices. The other threat is represented by the lack of stakeholders' training. In this case, besides the personal devices and the IoMTs, the asset affected by this threat is the newly design hardware.

5 Discussion

The purpose of this paper was to explore the supply chain of a Living Lab and identify its security and privacy challenges alongside with its vulnerabilities. This is the first paper, to our knowledge, to identify and present the dynamic supply chain of a Living Lab, the user requirements involved and to analyse the specific aspects of privacy and security, using PbD via the SecTro tool, in each phase of the supply chain. The reasoning behind this analysis was to take the research field one step further and for the findings to inform healthcare stakeholders and policy makers, regarding relevant mitigation strategies against malicious hacking actions.

5.1 Main findings and related work

The main findings of our study are outlined below:

- For the first time, the detailed supply chain of a Living Lab has been outlined and presented.
- Security and privacy challenges in a Living Lab have not been found in the literature from previous studies, until now.

- User requirements of a Living Lab have been identified according to their threat prevention, detection, and awareness.
- Relevant mitigation strategies are proposed (see next section).
- A complete and detailed model of the Living Lab has now been added to the literature.

There is a complete lack in the literature around exploring the privacy, security and vulnerability issues which are associated with the supply chain of a Living Lab. However, PbD is a field which has been identified as particularly important in recent years with several approaches within the literature. Therefore, we have adopted it in this paper as well.

More specifically, a recent review [38] has revealed 12 approaches associated with PbD, while an earlier review [39] has provided examples, at an abstract level, which are specific to the implementation of PbD in different fields. Work on the ontologies related to the PbD has also been conducted [40], without providing specific methods around it.

Previous studies which are closest to our approach include PriS [41] and socio-technical approaches related to security and privacy [42, 43]. The study by [41] proposes PriS, which is a goal-based approach, that outlines a clear process to support the mapping of relevant privacy requirements to privacy enhancing technologies via using privacy process patterns. Furthermore, the study by [42] presents a modelling framework which is inspired by the PbD principle to contribute to the design of GDPR compliant systems. Lastly, previous work of ours has modelled privacy and security requirements based on a proposed attacker's profile [43] and has also identified cybersecurity vulnerabilities and challenges in the supply chain of healthcare [44].

However, our proposal in this paper differs from the approaches which are found in the literature. Also, the fact that the Living Labs have not been explored at all on these issues has made them an ideal testbed. The requirements which are presented here are collected by real-world evidence, moving one step ahead from desk studies, and are modelled as such. Additionally, it is worth noting that the language which is used in the modelling (i.e., data breach, data minimisation) conceptualizes and supports core aspects of PbD as these are defined in the GDPR.

5.2 Implications

The modelling which is presented in this paper is to be understood as an opportunity to develop mitigation strategies for uprising security and privacy risks and as an extension of the existing codes of conduct, policies, and standards. It appears essential to produce this information flow to communicate to organizations and professional bodies the existing needs and provide some actions in order to prevent wrongful practices.

Practical awareness mitigation strategies, related to privacy and security issues in a Living Lab, which have been derived based on the findings of this study are proposed as follows:

- Keep a balance between the technical knowledge which is acquired by technicians and the background of the citizens by considering both their limitations, skills, and capabilities.
- Organize formal and informal meetings between all stakeholders involved in a Living Lab to manage the different views, expectations, and levels of knowledge.
- Arrange interactive and practical cybersecurity training for both citizens and professionals to ensure that the productions of services or goods not only improve individuals and community's quality of life but do so in a secure way.

- Both users and developers should manage and understand ethical implications which often arise during the process.
- Policies and standards should be made known to all stakeholders and relevant professionals (i.e., DPO) need to monitor that they are being followed.
- Behavioural and social scientists, and phycologists need to be involved when developing privacy and security standards to ensure that psychosocial, human, and behavioural aspects are considered.

5.3 Limitations and future research

It is important to keep in mind the limitations of this study. Firstly, due to the flexible and wide nature of a Living Lab, we may have missed stakeholders (actors), threats, goals, or constraints, in our analysis. Since there is no relevant literature identifying all aspects of this supply chain and due to the experimental nature of the study, we would propose future research to examine these relationships more extensively. The information has derived from our work in the Brighton and Hove Digital Health Living Lab, and it is possible that researchers from another Living Lab may have added or excluded some of the identified components. A second limitation involves the contextual and artificial context used in the study. The participants in this research were not contacted via surveys or interviews, the information was derived from the research team's long-lasting research experience with the Living Labs and the scarce evidence which were identified in the literature. Future studies are invited to search extensively all stakeholders and the perceived privacy and security risks. A third limitation is regarding the modelling which we performed of the Living Lab. This modelling needs to be supported by a holistic and complete evaluation framework and additional studies are encouraged to do so. As future work, our research team is planning to further extend the language used to provide support for related concepts, which are connected to PbD, for which there is currently limited support. Furthermore, we are planning to utilize and test the future automation provided by the SecTro tool, to take advantage of the modelling language concepts. We are keen to evaluate the automation which will allow us to automatically compare the models created with existing organisational data-related models, such as database schemas or entity diagrams, to emancipate organisations to automatically identify data minimisation breaches. Further technical mitigation strategies shall be proposed via personilised sector-specific frameworks addressing particular vulnerabilities respectively.

5.4 Conclusions

The main purpose of this study was to present the supply chain of a Living Lab and examine its related security and privacy issues via a thorough analysis. To our knowledge, this is the first paper in the literature which achieves this aim. A Living Lab, like any other ecosystem, has a plethora of cybersecurity issues that urgently require the proposal and application of mitigation strategies by both the users and the professionals involved. Additional work is needed to advance this field further.

Acknowledgments

The research conducted in this paper was triggered by the authors' involvement in the project 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) under grant agreement No 883273. The first author would also like to acknowledge the project 'Affective based integrated care for better quality of life' (TeNDER), funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 875325. The authors are grateful for the financial support of these projects that have received

funding from the European Union's Horizon 2020 research and innovation programme. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned projects.

References

[1] Department of Health and Human Services. Summary of the HIPAA privacy rule, May 2019. https://www.hhs.gov/hipaa/forprofessionals/privacy/laws-regulations/ [Online; Accessed on May 20, 2021].

[2] M. Muthupalapania and K. Stevenson. Healthcare cyber-attacks and the covid-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, 33(1):1–19, February 2020.

[3] ENISA. Cybersecurity in the healthcare sector during Covid-19 pandemic, May 2020. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic [Online; Accessed on June 12, 2021].

[4] Herjavek Group. The 2020 Healthcare Cybersecurity Report, December 2020. https://www.herjavecgroup.com/wp-content/uploads/2019/12/Healthcare-Cybersecurity-Report-2020.pdf [Online; Accessed on June 15, 2021].

[5] HIPPA. Healthcare Email Fraud Attacks Have Increased 473% in 2 Years, February 2021. https://www.hipaajournal.com/healthcare-email-fraud-attacks-have-increased-473-in-2-years/ [Online; Accessed on September 9, 2021].

[6] A.Sulleyman. NHS cyber-attack: why stolen medical information is so much more valuable than financial data, May 2017. https://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-sell-financial-a7733171.html [Online; Accessed on July 22, 2021].

[7] The CyberPeace Institute. Playing with lives: Cyberattacks on healthcare are attacks on people, March 2021. https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf [Online; Accessed on October 1, 2021].

[8] M. Van Geenhuizen. From ivory tower to living lab: Accelerating the use of university knowledge. *Environment and Planning C: Government and Policy*, 31(6):1115–1132, January 2013.

[9] J. Svensson, C.I. Eriksson, E. Ebbesson, and M. Åkesson. Methods and Techniques for User Contribution: Challenges from a Living Lab Perspective. Presented at the IRIS32, Information Systems Research Seminar in Scandinavia, August 2009. http://urn.kb.se/resolve?urn=urn:nbn:se:hh:diva-5059 [Online; Accessed on August 11, 2021].

[10] European Network of Living Labs. What are the living labs, 2020. https://enoll.org/about-us [Online; Accessed on July 3, 2021].

[11] M. Hossain, S. Leminen, and M. Westerlund. A systematic review of living lab literature. *Journal of cleaner production*, 213:976–988, March 2019.

[12] CIPS. What is a supply chain, 2020. https://www.cips.org/knowledge/procurement-topics-and-skills/supply-chain-management/what-is-a-supply-chain/ [Online; Accessed on August 29, 2021].

[13] S.D. Warren and L.D. Brandeis. The right to privacy. *Harvard Law Review*, 4(5):193–220, December 1890.

[14] R. Densmore. *Privacy Program Management: Tools for Managing Privacy Within Your Organization*. International Association of Privacy Professionals, 2013.

[15] Australian Government-Office of the Australian Information Commissioner. Privacy By Design, 2019. https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design/ [Online; Accessed on September 29, 2021].

[16] F. Semantha, S. Azam, K. Yeo, and B. Shanmugam. A systematic literature review on privacy by design in the healthcare sector. *Electronics*, 9(3):452–479, March 2020.

[17] Sibenco Legal & Advisory. Privacy and Data Breaches-How Information Governance Minimises the Risk, January 2019. http://www.infogovanz.com/privacy-and-data-breaches-how-information-governance-minimises-the-risk [Online; Accessed on November 10, 2021].

[18] A.H. Seh, M. Zarour, M. Alenezi, A.K. Sarkar, A. Agrawal, R. Kumar, and R.A. Khan. Healthcare data breaches: Insights and implications. *Healthcare*, 8(2):1–18, May 2020.

[19] ENISA. Healthcare's Cybersecurity Incident Response Spotlighted at European Security Event, November 2019. https://www.enisa.europa.eu/news/enisa-news/healthcare2019s-cybersecurity-incident-response-spotlighted-at-european-security-event [Online; Accessed on November 10, 2020].

[20] NIST. Incident Response: The Cynet 360 platform is the world's fastest IR tool and includes automated attack detection and remediation, 2021. https://www.cynet.com/incident-response/nist-incident-response/ [Online; Accessed on November 15, 2021].

[21] S.C. Kang. Initiation of the suan-lien living lab – a living lab with an elderly welfare focus. *International Journal of Automation and Smart Technology*, 2(3):189–199, September 2012.

[22] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider. Iot privacy and security: Challenges and solutions. *Applied Sciences*, 10(12):1–17, May 2020.

[23] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. Fontaine, A. Filippoupolitis, and E. Roesch. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, 78(1):398–428, September 2018.

[24] AI4HEALTHSEC. A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures, October 2020. https://cordis.europa.eu/project/id/883273 [Online; Accessed on November 15, 2021].

[25] H. Mouratidis. Secure software systems engineering: The secure tropos approach. *Journal of Software*, 6(3):331–339, March 2011.

[26] H. Mouratidis, N. Argyropoulos, and S. Shei. *Security Requirements Engineering for Cloud Computing: The Secure Tropos Approach*. Springer-Verlag, 2016.

[27] H. Mouratidis and P. Giorgini. Secure tropos: a security-oriented extension of the tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(2):385–309, April 2007.

[28] M. Pavlidis and S. Islam. Sectro: A case tool for modelling security in requirements engineering ssing secure tropos. In *Proc. of the 23th International Conference on Advanced Information Systems Engineering in Computer Science (CAiSE'11), London, United Kingdom*, volume 734 of *Lecture Notes in Computer Science*, pages 89–96. Springer-Verlag, December 2011.

[29] M. Pavlidis, H. Mouratidis, C. Gonzalez-Perez, and C. Kalloniatis. Addressing privacy and trust issues in cultural heritage modelling. In *Proc. of the 10th International Conference on Risks and Security of Internet and Systems in Risks and Security of Internet and Systems (CRiSIS'15), Mytilene, Greece*, volume 9572 of *Lecture Notes in Computer Science*, pages 3–16. Springer-Verlag, April 2016.

[30] M. Pavlidis, H. Mouratidis, and S. Islam. Modelling security using trust based concepts. *International Journal of Secure Software Engineering*, 2(3):36–53, April 2012.

[31] M. Pavlidis, H. Mouratidis, E. Panaousis, and N. Argyropoulos. Selecting security mechanisms in secure tropos. In *Proc. of the 7th ternational Conference on Trust and Privacy in Digital Business in Trust, Privacy and Security in Digital Business (TrustBus'17), Lyon, France*, volume 10442 of *Lecture Notes in Computer Science*, pages 99–114. Springer-Verlag, October 2017.

[32] Diamantopoulou V, K. Angelopoulos, J. Flake, A. Praitano, J.F. Ruiz, J. Jurjens, M. Pavlidis, D. Bonutto, A.C. Sanz, H. Mouratidis, J.G. Robles, and A.E. Tozzi. Privacy data management and awareness for public administrations: A case study from the healthcare domain. In *Proc. of the 17th Annual Privacy Forum in Privacy Technologies and Policy (APF'17), Jordan, Amman*, volume 10518 of *Lecture Notes in Computer Science*, pages 192–209. Springer-Verlag, October 2017.

[33] L. Piras, M.G. Al-Obeidallah, M. Pavlidis, H. Mouratidis, A. Tsohou, E. Magkos, and A. Praitano. A data scope management service to support privacy by design and gdpr compliance. *Journal of Data Intelligence*, 2(2):136–165, June 2021.

[34] L. Piras, M.G. Al-Obeidallah, A. Praitano, A. Tsohou, H. Mouratidis, B.G.N. Crespo, J.B. Bernard, M. Fiorani, E. Magkos, and A.C. Sanz. Defend architecture: A privacy by design platform for gdpr compliance. In *Proc. of the 16th International Conference on Trust and Privacy in Trust, Privacy and Security in Digital Business (TrustBus'19), Linza, Austria*, volume 11711 of *Lecture Notes in Computer Science*, pages 78–93. Springer-Verlag, August 2019.

[35] L. Piras, D. Dellagiacoma, A. Perini, A. Susi, P. Giorgini, and J. Mylopoulos. Design thinking and acceptance requirements for designing gamified software. In *Proc. of the 13th Intern. Confer. on Research Challenges in Information Science (RCIS'19), Brussels, Belgium*, pages 1–12. IEEE, May 2019.

[36] L. Piras, M. Pavlidis, H. Mouratidis, A. Tsohou, E. Magkos, A. Praitano, A. Iodice, and B. Crespo. Defend dsm: A data scope management service for model-based privacy by design gdpr compliance. In *Proc. of the 17th International Conference on Trust and Privacy in Trust, Privacy and Security in Digital Business (TrustBus'20), Bratislava, Slovakia*, volume 12395 of *Lecture Notes in Computer Science*, pages 186–201. Springer-Verlag, September 2020.

[37] A. Tsohou, E. Magkos, H. Mouratidis, G. Chrysoloras, L. Piras, M. Pavlidis, J. Debussche, M. Rotoloni, and B.G.N. Crespo. Privacy, security, legal and technology acceptance elicited and consolidated requirements for a gdpr compliance platform. *Information & Computer Security*, 28(4):531–553, April 2020.

[38] B. Kostova, S. Gurses, C, and Troncoso. Privacy engineering meets software engineering. on the challenges of engineering privacy by design. *Journal of arxiv*, July 2020.

[39] A. Romanou. The necessity of the implementation of privacy by design in sectors where data protection concerns arise. *Computer law & security review*, 34(1):99–110, February 2018.

[40] M. Gharib, P. Giorgini, and J. Mylopoulos. Ontologies for privacy requirements engineering: A systematic literature review. *Journal of Computing Reasearch Repository*, pages 1–74, November 2016.

[41] C. Kalloniatis, E. Kavakli, and S. Gritzalis. Addressing privacy requirements in system design: the pris method. requirements engineering. *Requirements Enginnering*, 13(3):241–255, August 2008.

[42] M. Robol, M. Salnitri, and P. Giorgini. Toward gdpr- compliant socio-technical systems: Modeling language and reasoning framework. In *Proc. of the 10th IFIP Working Conference on The Practice of Enterprise Modeling (PoEM'17), Leuven, Belgium*, volume 305 of *Lecture Notes in Business Information Processing*, pages 236–250. Springer-Verlag, November 2017.

[43] K. Kioskli and N. Polemi. A socio-technical approach to cyber risk assessment. *World Academy of Science, Engineering and Technology International Journal of Electrical and Computer Engineering*, 14(10):305–309, December 2020.

[44] K. Kioskli, T. Fotis, and H. Mouratidis. The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. In *Proc. of the the 16th International Conference on Availability, Reliability and Security on SecHealth Workshop (ARES'21), Vienna, Austria*, pages 1–19. ACM, August 2021.

Author Biography

Kitty Kioskli has received a B.Sc. in Social Anthropology from Panteion University, an M.Sc. in Health Psychology from City, University of London, and a Ph.D. in Health Psychology from King's College London. Her PhD was fully funded under a nationally competitive fellowship from Diabetes UK. Currently, Dr Kioskli is working as a Research Fellow at the University of Essex and as a Project Manager at Gruppo Maggioli. She has also co-founded trustilio B.V. a start-up consultancy providing services in cybersecurity, behaviour-change, business and research innovation where she acts as the CEO. Her research interests lie in the areas of cybersecurity, digital health, behaviour change, psychosocial and human factors. She is the author of a number of high-impact peer-reviewed publications, has presented in several national and international conferences and has received 4 awards

in these fields. Meanwhile, she serves as an editorial review board member in a number of high-impact journals. She has also worked as a postdoctoral research fellow at City, University of London and University of Brighton, as a graduate teaching assistant at King's College London and as a PhD tutor at the Brilliant Club. Finally, Dr Kioskli has served as a researcher in a plethora of European and national R&D projects.

Daniele Dellagiacoma has received both a B.Sc. and a M.Sc. in Computer Science from the University of Trento (Italy). After the University he had working experiences in both academic and industrial environments. He worked on several European and national research projects. Moreover, he is the author of some peer-reviewed publications, and he presented them in few international conferences. He worked as a Research Fellow at the University of Brighton whereas he is currently the team leader of the R&D department in Delta Informatica S.p.A., coordinating the technical aspects of a national research project.

Theofanis Fotis, Air Force Officer Nurse veteran, is a Principal Lecturer at the School of Health Sciences and Assistant Director Outreach of the Centre for Secure, Intelligent and Usable Systems (CSIUS) at the University of Brighton.He is Fellow of the Higher Education Academy (HEA), Editor in Chief of the British Journal of Anaesthetic and Recovery Nursing (BJARN) and a visiting researcher at the School of Nursing, Hong Kong Polytechnic University. He is currently the Academic Lead of the Brighton and Hove Digital Health Living Lab, where citizens, health professionals and industry are working side by side on health innovation through co-creation. The project has been included in the National Initiative MADEatUNI, as one of the 100+ leading ways universities are saving lives and keeping the public healthy, creating healthier lifestyles and a fairer society. Theo is an international scholar in the health sciences with h-index 11 and over 300 citations and his funding portfolio includes Horizon2020, Interreg2Seas, Health Education England, AHSN and AfPP. In 2015 he used the term 'Digital Nursing', to define a future workforce of health care practitioners with the specialised knowledge and skills to utilise digital technologies for patient and citizen benefit. As a recognition of his work, in 2018 he was named one of the Top 50 Healthcare IT leaders in Europe by the Healthcare Information and Management Systems Society (HIMSS Europe), the largest health IT membership organisation in the world. He is active member of international bodies and committees including the International Task Force for Technology Informatics Guiding Education Reform (TIGER HIMSS International), the Cybersecurity Privacy and Security committee (HIMMSS International) and the Phi Mu Chapter of the Sigma Theta Tau International Honour Society of Nursing. He has extensive experience of acting as evaluator for national and international funding bodies including EPSRC, NIHR, UK Research and Innovation (UKRI) and the Hong Kong Research Grants Council. In addition, he acts as an external evaluator for Higher Education quality assurance organisations, including the National Commission for Academic Accreditation and Assessment (NCAAA) of Saudi Arabia and the Commission for Academic Accreditation (CAA) of United Arab Emirates.

Haralambos Mouratidis is Professor of Software Systems Engineering and founding Director of the Centre for Secure, Intelligent and Usable Systems (CSIUS) at the University of Brighton. He is Fellow of the Higher Education Academy, and a visiting professor at the University of Ionian (Greece). His research interests lie in the intersection of security, privacy, and software engineering. He has pioneered work in developing methodologies, modelling languages, ontologies, tools and platforms to support the analysis, design, and monitoring of security, privacy, risk and trust for large-scale complex software systems. He has applied his theoretical work to practical applications in domains such as critical infrastructures, cloud computing, healthcare, telecommunications, banking, and e-commerce. He has published more than 150 papers (h- index 30) and he has led and/or participated in projects funded by the European Union (FP7, Horizon2020), EPSRC, the Royal Academy of Engineering, the Higher Education Funding Council of England (HEFCE), and the Japanese National Institute of Informatics to name few of the funders. He has also received funding for knowledge exchange and industrial projects from Innovate UK, the European Regional Development Fund, British Telecom, ELC, Powerchex, and FORD. He has strong experience of acting as evaluator for national and international funding bodies including the EPSRC, HEA, the EU, and various national councils and he has acted as invited subject expert for events organised by the EU, NATO and Innovate UK. He is member of working groups at ERCIM, IFIP and national initiatives related to security, privacy and trust.

Appendix A User requirements as derived from AI4HEALTHSEC project [24]

User ReqID	Description
REQ1	The risk assessment /management models and process shall be considered from a holistic view of internal (i.e., organisational, technical, medical devices) and external context of the complex health care system.
REQ2	The introduction of risk assessment/management models and processes in the AI4HEALTHSEC methodology shall adequately take into account the complexity of the ICT infrastructure and technical evolution of medical devices that underpin security processes of health care complex adaptive system.
REQ3	The risk management approach shall provide an informed real time decision making for managing cyber security risks and ensuring overall business continuity.
REQ4	The methodology shall define the organisation cyber security needs, risk appetite, and risk tolerance for the key healthcare ICT infrastructure areas.
REQ5	The risk assessment/management approach shall alleviate the limitations of existing risk management methodologies in terms of their ability to deal with ICT systems in the critical infrastructures.
REQ6	The methodology shall leverage, use, and implement existing cyber security, information security risk management, information security incident management standards including ISO 31000, ISO27001, ISO 27005, ISO 27031, and ISO 27032 associated with the protection of the complex ICT infrastructure.
REQ7	The methodology shall offer compliance with the relevant regulation necessary to compliance with the health care information system sector.
REQ8	The methodology shall automatically detect potential cyber-attack and adversary actions using autonomous intelligence swarm agents and reporting to the supervisor agents, so that evidence are combined and correlated with the existing data for the attack predication and new attack vector discovery.
REQ9	The methodology shall include a real time communication, interaction, and feedback among hierarchy-based multiple agents including supervisor and swarm agents and create an overall dynamic cyber security situational awareness.
REQ10	The methodology and associated risk management framework shall consider organisation-wide vulnerabilities detection using collective behaviour of swarm intelligence taking into account the underlying complexity of the ICT infrastructure and interoperability and interconnectivity among various subcomponents including medical devices.
REQ11	The methodology shall consider depth of access by measuring how far threat actors reach within the ICT infrastructure by collective swarm intelligence data for the risk identification and predication.
REQ12	The methodology shall introduce a risk management system, which will consider the nature and interdependencies of cybersecurity and medical assets and as well as their implications on overall business continuity.
REQ13	The methodology shall adopt an evidence-driven Cyber Security Risk Assessment model in order to capture and deal with cascading effects of risks, threats and vulnerabilities, associated with the health care ICT infrastructure.

REQ14	The methodology shall help elicit, understand and analyse risk management requirements for the health care ICT infrastructure, with particular emphasis on requirements associated with the overall complex system and its supply chain context.
REQ15	The methodology shall consider all organisation wide vulnerabilities by correlating data from the swarm agents and its impact for the net risk calculation.
REQ16	The risk assessment approach should follow quantitative assessment methods to determine the risk level, based on existing consistent cyber security threat data.
REQ17	The risk assessment approach should consider Cyber Threat Intelligence (CTI) information including relevant threat actors, their capabilities, skills, motivations, and underlying TTP and IoC.
REQ18	The methodology should consider cyber risk modelling considering assets and their dependencies, vulnerabilities within the assets, possible attack paths, threat intelligence properties, and risks.
REQ19	The methodology should leverage simulation models combined with a multi–criteria decision making approach in order to produce timely, accurate, relevant and high-quality evidence, information, indicators, factors and parameters associated based on which the multi-dimensional risks will be assessed.
REQ20	The methodology should use graphs to discover and represent possible attacks plans and patterns and will adopt a general approach to integrate several aspects of both vulnerabilities and threat agents.
REQ21	The methodology should identify and model assets, processes, risks, stakeholders' relationships/interactions and dependencies.
REQ22	The methodology shall create a range of metrics covering reliability, credibility, acceptance, timeliness, realism of risk management goals and the level of integration of the risk management approach in decision making structures. These metrics should be able to be measured across all cyber-security assets, medical device, and ICT systems available within health care infrastructure.
REQ23	The methodology shall determine the level of assurance based on the evidence of existing controls and their effectiveness and recommend alternative courses of action for responding to risks.
REQ24	The methodology shall explore new techniques/methods for the credible calculation of insurance premiums.
REQ25	The risk management approach shall ensure the constant vigilance of existing risks, by offering mechanisms to understand status of residual value of risk and identifying any new risk using intelligence swarm agents.
REQ26	The risk analysis methodology shall provide real-time decision-making support for incident response and post incident review activities.
REQ27	The risk identification, forecasting and analyse shall provide a better understanding of the cyber security incident related information.
REQ28	The risk management methodology shall align with the incident response and post-incident activities to ensure eradication of the threats and risks and overall business continuity.
REQ29	The risk assessment methodology should support threat intelligence information and incident response planning, through lessons learn from the evolving threats, risks and related incidents.

REQ30	The risk management methodology shall consider publishing best practices that include blueprints and guidelines for adapting the approach to other critical infrastructures sector, such as smart grid cyber physical systems.
REQ31	The project shall contribute best practices associated with the deployment and operation of its framework for risk management in health care sector of any type and size.
REQ32	The incident handling methodology shall support evidence collection on both real time and historic data from the various evidence collection sources to assist incident detection.
REQ33	The evidence collection process shall include batch data including, but not limited to, log files from vulnerable systems and network traffic.
REQ34	The evidence collection process shall include configurable steps, allowing for the specification of the type, format, and location of the incoming data sources.
REQ35	The evidence collection process shall consider anonymization of raw data collected by various sources. The platform needs a process to pseudo-anonymise or anonymise the collected data from various sources.
REQ36	The evidence preparation process shall consider the semi-structured nature of different datasets.
REQ37	The data collected shall include records about network usage and bandwidth and should allow the identification of network traffic anomalies and excessive bandwidth usage.
REQ38	The data collection process shall consider and be aligned with existing industry proprietary or non-proprietary data exchange protocols, with interest in understanding to some extent the messages exchanged, like network packages and messages from the interaction among systems.
REQ39	The incident handling process should be able to monitor the availability of signals and system web sources or services and calculate their response time for further analysis.
REQ40	The incident handling approach shall support normalization and transformation of raw data coming from semantically relevant sources to facilitate system independent data processing and sharing across the AI4HEALTHSEC Framework.
REQ41	The incident handling approach shall consider for managing structural and semantic mismatches across the different datasets collected.
REQ42	The incident handling approach shall support normalization and transformation for the unified representation of cyber security threats detected by internal or external components of this platform.
REQ43	The evidence preparation process shall support preliminary filtering of raw data, using predefined criteria over the parameters collected from raw data, so that irrelevant one can be removed and/or not taken into consideration in the incident handling process.
REQ44	The incident detection and event analysis approach shall be able to process streaming, batch and historic data.
REQ45	The incident detection and event analysis approach shall consider data uncertainty and incompleteness, so that the processing of the provided raw data can be feasible even in the absence of some elements.
REQ46	The organization and filtering of the incoming raw data (across all the available data sources) is essential for the further analysis of the current status of the systems. During this process the evidence chains would be generated, and the relevant data would be collected and stored for latter usage.

REQ47	The incident detection and event analysis approach shall support the preliminary analysis of relevant raw data to identify potential security incidents.
REQ48	The security event analysis approach shall support semantic and structural decisions regarding the description of the different type of incidents so that further processing of the information generated can be processable and meaningful.
REQ49	The incident detection and event analysis approach shall utilize existing knowledge sources with security data for correlating evidence to incidents and security events.
REQ50	The incident detection and event analysis approach should be customizable to further domains, other than health ICT infrastructures.
REQ51	The incident handling methodology should maintain a knowledge base with information about actual successful attack scenarios.
REQ52	The incident detection and event analysis approach should support decision making, towards developing more efficient and effective defence strategies, based on evidence from past detected incidents, extracted from the knowledge base.
REQ53	The incident handling methodology must provide cyber-attacks related information that can be shared with other organizations in a secure and privacy preserving way.
REQ54	The incident handling methodology must identify the attacks and related information.
REQ55	The incident handling methodology should be able to predict scenarios of attacks.
REQ56	The incident handling methodology should provide a visual representation of the cyber-attack path.
REQ57	The incident handling methodology should assure an acceptable risk level for the co-operating stakeholders.
REQ58	The incident handling methodology should promote defensive capabilities and provide a rational decision-making to help stakeholders in determining which security controls must be implemented to encounter the identified security issues and cyber-risks.
REQ59	The incident handling methodology should support matching evidence collected in real time with archived information for cyber-attack scenarios.
REQ60	The incident handling methodology shall be able to provide comparison among the patterns of data collected at the infrastructure nodes and the normal state of operations.
REQ61	The incident handling methodology shall allow decision makers in predicting the assets that are exposed to risks when a security event is detected.
REQ62	The incident handling methodology shall support decision makers in exploring different attack scenarios on potential harmfulness of a detected anomaly to the infrastructure.
REQ63	The incident handling methodology shall present the attack path of a detected incident across all impacted assets.
REQ64	The incident handling methodology shall present sufficient information to decision makers to enable them to understand the risk of cyber-attacks detected in real time on the infrastructure.
REQ65	The incident handling methodology shall always provide decision makers with access to the results of the risk assessment process to understand the consequences of a detected cyber-attack.
REQ66	The incident handling methodology shall provide recommendations to decision makers on the most suitable security controls to mitigate the risks from detected security events and cyber risks.

REQ67	The incident handling methodology shall allow decision makers understand the impact from the implementation of a defensive mechanism to support informed decisions when selecting the appropriate security controls.

Appendix B User requirements of a Living Lab according to their threat prevention, detection, and awareness

Threat Prevention	**Threat Detection**	**Threat Awareness**
The introduction of risk assessment/management models and processes in the AI4HEALTHSEC methodology shall adequately take into account the complexity of the ICT infrastructure and technical evolution of medical devices that underpin security processes of health care complex adaptive system.	The methodology shall automatically detect potential cyberattack and adversary actions using autonomous intelligence swarm agents and reporting to the supervisor agents, so that evidence are combined and correlated with the existing data for the attack predication and new attack vector discovery.	The risk management methodology shall align with the incident response and post-incident activities to ensure eradication of the threats and risks and overall business continuity.
The methodology shall define the organisation cyber security needs, risk appetite, and risk tolerance for the key healthcare ICT infrastructure areas.	The methodology shall include a real time communication, interaction, and feedback among hierarchy-based multiple agents including supervisor and swarm agents and create an overall dynamic cyber security situational awareness.	The risk assessment methodology should support updating threat intelligence information and incident response planning, through lessons learn from the evolving threats, risks, and related incidents.
The risk assessment /management approach shall alleviate the limitations of existing risk management methodologies in terms of their ability to deal with ICT systems in the critical infrastructures.	The methodology shall consider depth of access by measuring how far threat actors reach within the ICT infrastructure by collective swarm intelligence data for the risk identification and predication.	The risk management methodology shall consider publishing best practices that include blueprints and guidelines for adapting the approach to other critical infrastructures sector, such as smart grid cyber physical systems.

The methodology shall leverage, use and implement existing cyber security, information security risk management, information security incident management standards including ISO 31000, ISO27001, ISO 27005, ISO 27031, and ISO 27032 associated with the protection of the complex ICT infrastructure.	The risk identification, forecasting and analyse shall provide a better understanding of the cyber security incident related information.	The evidence preparation process shall support preliminary filtering of raw data, using predefined criteria over the parameters collected from raw data, so that irrelevant one can be removed and/or not taken into consideration in the incident handling process.
The methodology shall offer compliance with the relevant regulation necessary to compliance with the health care information system sector.	The incident handling process should be able to monitor the availability of signals and system web sources or services and calculate their response time for further analysis.	The organization and filtering of the incoming raw data (across all the available data sources) is essential for the further analysis of the status of the systems. During this process the evidence chains would be generated, and the relevant data would be collected and stored for latter usage.
The methodology and risk management framework shall consider organisation-wide vulnerabilities detection using collective behaviour of swarm intelligence considering the underlying complexity of the ICT infrastructure and interoperability and interconnectivity among subcomponents including medical devices.	The incident handling approach shall support normalization and transformation of raw data coming from semantically relevant sources to facilitate system independent data processing and sharing across the AI4HEALTHSEC Framework.	The security event analysis approach shall support semantic and structural decisions regarding the description of the different type of incidents so that further processing of the information generated can be processable and meaningful.
The methodology shall introduce a risk management system, which will consider the nature and interdependencies of cybersecurity and medical assets and as well as their implications on overall business continuity.	The incident handling approach shall consider for managing structural and semantic mismatches across the different datasets collected.	The incident handling methodology should maintain a knowledge base with information about actual successful attack scenarios.

The methodology shall adopt an evidence-driven Cyber Security Risk Assessment model in order to capture and deal with cascading effects of risks, threats and vulnerabilities, associated with the health care ICT infrastructure.	The incident handling approach shall support normalization and transformation for the unified representation of cyber security threats detected by internal or external components of this platform.	The incident handling methodology must provide cyber-attacks related information that can be shared with other organizations in a secure and privacy preserving way.
The methodology shall help elicit, understand and analyse risk management requirements for the health care ICT infrastructure, with particular emphasis on requirements associated with the overall complex system and its supply chain context.	The incident detection and event analysis approach shall support the preliminary analysis of relevant raw data (e.g., deviation from normal patterns) to identify potential security incidents.	The incident handling methodology shall present the attack path of a detected incident across all impacted assets.
The methodology shall consider all organisation wide vulnerabilities by correlating data from the swarm agents and its impact for the net risk calculation.	The incident detection and event analysis approach shall utilize existing knowledge sources with security data (either external knowledge used for training purposes or other security relevant knowledge acquired by other modules of this system) for correlating evidence to incidents and security events.	The incident handling methodology shall provide recommendations to decision makers on the most suitable security controls to mitigate the risks from detected security events and cyber risks.
The risk assessment approach should follow quantitative assessment methods to determine the risk level, based on existing consistent cyber security threat data.	-	-
The risk assessment approach should consider Cyber Threat Intelligence (CTI) information including relevant threat actors, their capabilities, skills, motivations, and underlying TTP and IoC.	-	-

The methodology should consider cyber risk modelling considering assets and their dependencies, vulnerabilities within the assets, possible attack paths, threat intelligence properties, and risks.	-	-
The methodology should leverage simulation models combined with a multi–criteria decision making approach in order to produce timely, accurate, relevant and high-quality evidence, information, indicators, factors and parameters associated based on which the multi-dimensional risks will be assessed.	-	-
The methodology should use graphs to discover and represent possible attacks plans and patterns and will adopt a general approach to integrate several aspects of both vulnerabilities and threat agents.	-	-
The methodology should identify and model assets, processes, risks, stakeholders' relationships/interactions and dependencies.	-	-
The methodology shall determine the level of assurance based on the evidence of existing controls and their effectiveness and recommend alternative courses of action for responding to risks.	-	-
The risk management approach shall ensure the constant vigilance of existing risks, by offering mechanisms to understand status of residual value of risk and identifying any new risk using intelligence swarm agents.	-	-

The incident handling methodology shall support evidence collection on both real time and historic data from the various evidence collection sources to assist incident detection.	-	-
The evidence collection process shall include batch data (i.e., collection of raw data over a specific period), including, but not limited to, log files from vulnerable systems and network traffic.	-	-
The evidence collection process shall include configurable steps, allowing for the specification of the type, format and location of the incoming data sources such as log files.	-	-
The evidence collection process shall consider anonymization of raw data collected by various sources. The platform needs a process to pseudo-anonymise or anonymise the collected data from various sources.	-	-
The evidence preparation process shall consider the semi-structured nature of different datasets.	-	-
The data collected shall include records about network usage and bandwidth and should allow the identification of network traffic anomalies and excessive bandwidth usage.	-	-

The data collection process shall consider and be at least partially aligned with existing industry proprietary or non-proprietary data exchange protocols, with particular interest in understanding to some extent the messages exchanged, including network packages and messages from the interaction among systems.	-	-
The incident detection and event analysis approach shall be able to process streaming, batch and historic data.	-	-
The incident detection and event analysis approach shall consider data uncertainty and incompleteness, so that the processing of the provided raw data can be feasible even in the absence of some elements.	-	-
The incident detection and event analysis approach should be customizable to further domains, other than health ICT infrastructures.	-	-
The incident handling methodology must identify the ongoing attacks and related information at all times.	-	-
The incident handling methodology should be able to predict possible scenarios of future attacks.	-	-
The incident handling methodology should assure an acceptable risk level for the cooperating stakeholders.	-	-