applied sciences

MDPI

Article

Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach

Marc Jofre [1], Diana Navarro-Llobet [1,*], Ramon Agulló [2], Jordi Puig [2], Gustavo Gonzalez-Granadillo [3], Juan Mora Zamorano [4] and Ramon Romeu [2]

[1] Department of Research and Innovation, Fundació Privada Hospital Asil de Granollers, 08402 Granollers, Barcelona, Spain; mjofre@fphag.org
[2] Digital Strategy Direction, Fundació Privada Hospital Asil de Granollers, 08402 Granollers, Barcelona, Spain; ragullov@fphag.org (R.A.); jpuig@fphag.org (J.P.); rromeu@fphag.org (R.R.)
[3] Atos Research & Innovation, Cybersecurity Laboratory, 08020 Barcelona, Barcelona, Spain; gustavo.gonzalez@atos.net
[4] Instituto de Invest, Sanitaria Puerta de Hierro, Servicio Madrileño de Salud, Majadahonda, 28222 Madrid, Madrid, Spain; jmora@idiphim.org
* Correspondence: diananavarro@fphag.org

Abstract: Point-of-care systems are generally used in healthcare to respond rapidly and prevent critical health conditions. Hence, POC systems often handle personal health information; and consequently, their cybersecurity and privacy requirements are of crucial importance. While, assessing these requirements is a significant task. In this work, we propose a use case approach to assess specifications of cybersecurity and privacy requirements of POC systems in a structured and self-contained form. Such an approach is appropriate since use cases are one of the most common means adopted by developers to derive requirements. As a result, we detail a use case approach in the framework of a real-based healthcare IT infrastructure that includes a health information system, integration engines, application servers, web services, medical devices, smartphone apps and medical modalities (all data simulated) together with the interaction with participants. Since our use case also sustains the analysis of cybersecurity and privacy risks in different threat scenarios, it also supports decision making and the analysis of compliance considerations.

Keywords: cybersecurity; healthcare; incidents; information privacy; IT infrastructure; point-of-care; risk assessment; sensitive medical data; threats; use case

Citation: Jofre, M.; Navarro-Llobet, D.; Agulló, R.; Puig, J.; Gonzalez-Granadillo, G.; Mora Zamorano, J.; Romeu, R. Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. *Appl. Sci.* **2021**, *11*, 6699. https://doi.org/10.3390/app11156699

Academic Editor: Hassan Chizari

Received: 9 June 2021
Accepted: 19 July 2021
Published: 21 July 2021

1. Introduction

Cybersecurity and privacy incidents are a growing threat to the healthcare industry in general, and hospitals in particular [1]. The healthcare industry has lagged behind other industries in protecting its main stakeholders (e.g., care staff and patients), and now hospitals must invest considerable capital and effort in protecting their IT systems [2]. However, moving to more protected and resilient digital infrastructures in healthcare is a challenge because hospitals are extraordinary technology-saturated, complex organizations with high end-point complexity, internal politics, and regulatory pressures. Therefore, healthcare organizations of all types looking to grow and achieve their financial, quality, service and compliance performance objectives must understand and account for the capabilities, drivers, strategies, and challenges of other ecosystems such as cybersecurity and information privacy. Hence, as cybersecurity and privacy become more of a priority for hospitals, it is essential a holistically integration in the different processes, components and stages influencing the healthcare ecosystem.

One relevant aspect to consider regarding cybersecurity and privacy risks are healthcare point-of-care (POC) systems which have been widely used in hospitals in order to provide innovative solutions to medical professionals. Where, POC systems provide an

overview of the patients' conditions in a way that makes it easier for professionals to respond on time and prevent critical situations. POC systems are platforms that incorporate devices and applications in order to collect, process and visualize data. Using large amounts of data, which contain personal health information and sensitive medical data, communicated across various POC systems, backend analytical platforms, user workstations and smartphones, it becomes evident that there are multiple threats that may cause data leakages or breach incidents. Naturally, these platforms create and expanded attack surface, which may be challenging to identify and address. Hospitals and care centers need to address these threats by efficiently assessing the associated risks and mitigate them with the proper cybersecurity and privacy safeguards.

Namely, POC systems can be categorized in three classes according to their usage model [3] (i) for testing and diagnostic applications (e.g., medical devices), (ii) for patient monitoring (e.g., smartphone apps) and (iii) for as interfacing with other devices (e.g., web-based services and integration servers). Hence, considering the latter classes, some common associated threats to POC systems encompass legacy operating systems and software, lack of timely software updates and patches, medical devices not having basic security features, insecure implementation of web-services, lack of awareness of cybersecurity and privacy issues and limited power and resources [4], among others. Typically, these threats can be exploited by several common attacks (e.g., cross-site scripting, Structured Query Language (SQL) or Extensible Markup Language (XML) injection, client-side attacks, malware and denial-of-service).

Generally, risk is defined as the combined probability of an unwanted event and its level of impact. It is described as a function of the probability that a given source of threat exerts a potential vulnerability and the consequent impact of this adverse event on the organization [5]. Cybersecurity risk, also known as information technology risk, is the new management challenge of the third millennium; it affects the information and technology assets of organizations. On one hand, cybersecurity risk is defined in [6] as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems". In particular, a cybersecurity threat is a potential attack that exploits a vulnerability of the system to cause damage, whilst a threat scenario is a flow of events or attacks containing interactions between a malicious actor and a system to cause damage. On the other hand, privacy risk assessment as indicated in [7] aims to "analyze and quantify the privacy risks associated with new systems". Accordingly, considerable research has been devoted to eliciting and analyzing cybersecurity and privacy risk assessment [6–10]. However, the applicability of these approaches in the context of cybersecurity and privacy risk assessment modeling for POC systems in healthcare ecosystems shows limitations with respect to (i) their support for explicitly specifying various types of cybersecurity threats, (ii) the definition of threat scenarios and (iii) the specification of mitigation and preventing actions (e.g., cyber hygiene) for these threats.

Moreover, the above risks have to be properly communicated and accounted in the overall operational structure of organizations. For instance, in business, financial value may be acceptable as the ultimate unit, which is used to quantify direct cost—even reputation and human lives. However, certainly the healthcare sector does not only operate on a competitive or financial basis, and may prefer units that more closely relate to the concept of privacy risk. Therefore, to assess the cybersecurity requirements of POC systems, it is necessary to take into consideration the characteristics of the specific service being developed and of the device types on which the service is going to be deployed.

Accordingly, use cases are one of the most common means adopted by software engineers and end-users to elicit requirements because they ease the communication between stakeholders to assess specific requirements [11]. Additionally, to achieve widespread applicability, the need for integrating cybersecurity and privacy requirements with use case modeling warrants the development of reusable templates in different applications, and in particular for healthcare applications. Systematic approaches to eliciting cybersecurity

requirements based on use cases, with emphasis on description and methods guidelines have been proposed [12]. However, existing approaches lack reusable templates for misuse cases, as opposed to only well behaving use cases [12–15]. However, with slight modifications, use cases can aid the integration of misuse case scenarios, with functional and non-functional requirements, when considering cybersecurity and privacy risk [16].

In the direction to remediate the limitations described above, we propose a use case approach, including misuse cases, in the framework of a real-based healthcare IT infrastructure for POC cybersecurity and privacy risk assessment. In particular, the objectives of this work are to (i) detail a use case that sustains the specifications of cybersecurity and privacy requirements, (ii) address the above challenges by including the modelling based on risk management capability model (RMCM), and (iii) produce an approach tailored to accounting POC in healthcare ecosystems. In this regard, the paper is organized as follows. Section 2 introduces the context of our use case approach and proposed scenarios, compared to the state-of-the-art, to provide the motivations behind POC systems in healthcare. Sections 3 and 4 describe the technical developments, proposed pilot plan and risk assessment capability for POC use cases in healthcare environments, respectively. This is followed by Section 5, which discusses the results connected with the outcomes in several dimensions of cybersecurity and privacy risks. Finally, Section 6 summarizes the work, provides conclusions, and proposes future research.

2. Proposed Use Case Overview

The work presented in this article has been develop as part of a European Union (EU) project Secure and Private Health Data Exchange (CUREX) [17–19], which is developing a software platform aimed at delivering trust-enhancing, secure, and private-by-design systems and applications for the healthcare domain. In general, CUREX delivers specific cybersecurity and privacy risk solutions based on the following set of measurable objectives: (i) to deliver tools for assessing cybersecurity and privacy risks associated with health data exchange, (ii) to deliver a decision support tool for devising optimal cybersecurity and privacy safeguards, (iii) to deliver a Blockchain-based platform for enhancing trust in health data exchange, (iv) to enhance cyber hygiene in healthcare organizations, (v) to demonstrate the value of the CUREX platform through proof-of-concept use cases, and (vi) to conduct techno-economic, market and legal analysis and propose business and application models. In order to accomplish these objectives, the project brings academic institutions, healthcare end-users and software development companies together in a consortium to enhance the pool of available resources with partners and competitors to leverage technology development with high impact. Therefore, in conjunction with optimal recommended safeguards, CUREX delivers targeted measures for raising the cyber hygiene of healthcare organizations through the recommendation of strategies and methodologies for training and raising awareness activities, targeted towards healthcare employees (administration, medical, and IT personnel) on cybersecurity and privacy risks incurred during data exchange [20]. Training will involve the development of cybersecurity defending skills, e.g., empowering social engineering defenses [21]. In this way, healthcare employees will feel more confident in handling and exchanging sensitive data and improve their capabilities to perform their daily professional tasks effectively and in a secure fashion.

Particularly, as elucidated in the previous section, we will center this work in the development of a use case (also with misuse case extensions) to assess the cybersecurity and privacy risks in POC systems, together with remediation actions based on cyber hygiene recommendations, for different target groups of healthcare professionals at Fundació Privada Hospital Asil de Granollers (FPHAG) hospital. Contextualizing, FPHAG is a health and healthcare provider center of the public integral health system of Catalonia (SISCAT) of the Catalan health system, shown in Figure 1a. The hospital provides healthcare assistance both for acute and non-acute patients and it is the reference hospital of the territories comprising the area known as Vallès Oriental (Barcelona), covering a population of around 400,000 people and with a total number of 340 beds.

In the described context, considering data from August 2019, FPHAG's information network infrastructure was subject to more than 6000 different malware and intrusion attacks during a period of a year. Malware attack incidents were classified as: 205 viruses, 500 spywares, 189 adware and 2490 botnet attacks. Where these intrusion attack incidents' risk levels were classified as: 19 critical, 8 severe, 1876 average and 718 as low intensity level; and all the attacks were blocked or handled by the firewall. The latter statistics, all with positive outcome, are of relevance and point that correct infrastructure protection and IT-best-practices are in place at FPHAG. Nevertheless, still these are external attacks (blocked by the firewall), while instead internal attacks are very valuable to assess in a use case approach. First, because they are less frequent, and secondly because they can produce a catastrophic outcome. Therefore, a complete independent infrastructure similar to the real IT infrastructure of the hospital has been designed and develop at FPHAG, to work with these potential attacks in a use case approach, to assess requirements for testing and improving the CUREX platform solution, as shown in Figure 1b. Accordingly, the develop experimental IT infrastructure is composed of (i) a health information system (HIS) framework, containing file systems, a database and an image server; (ii) web integration server and services; and (iii) three different groups of POC systems: files of clinical history stored in the HIS as pdf, doc and structured data files; a patient smartphone app; and medical devices consisting of an electrocardiogram (EC), a ultrasound machine (US) and a CT-scan modality simulator (emulated medical device). All the personal and health data generated and stored with the different components is simulated, hence no real data from patients has been used.

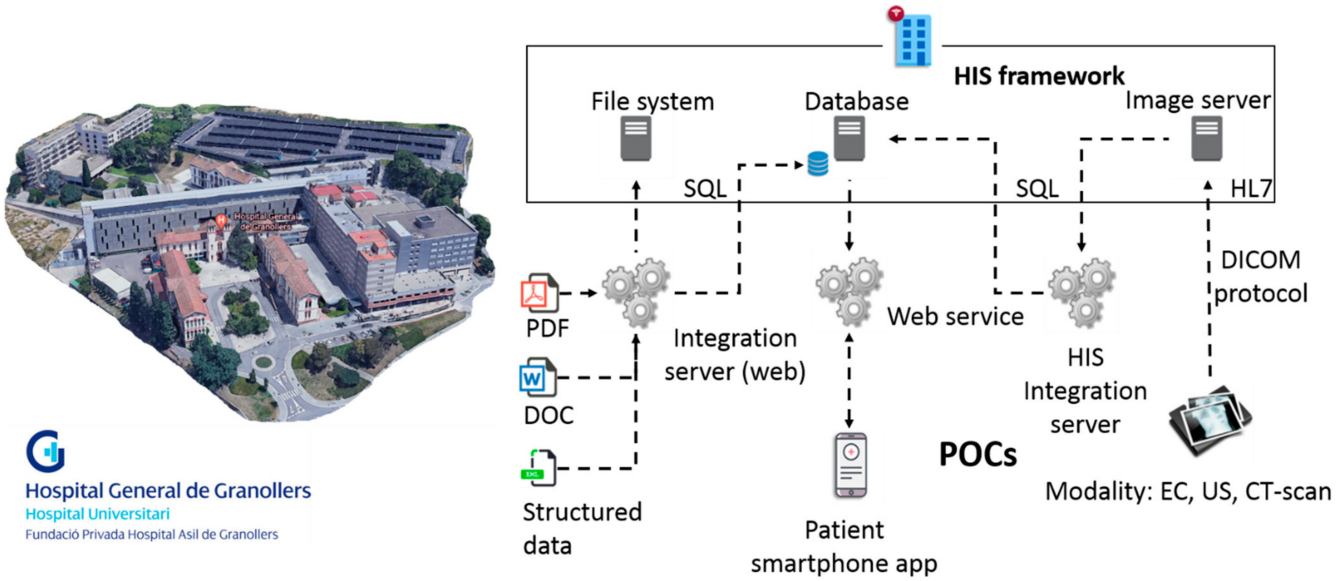

Figure 1. The experimental infrastructure has been designed and develop at FPHAG. (**a**) FPHAG facilities' view including: Granollers General Hospital, Adolfo Montañá Geriatric, the Knowledge Building and the surrounding facilities and services. (**b**) Topological representation of the IT infrastructure designed and develop to support the use case approach.

With the above-described points, the scope of the proposed use case in this work assumes the situation that "the hospital IT department has raised concerns about the cybersecurity issues that may emerge from the operation and the communication of the clinical data handled with POC systems. Indeed, since the data contains highly sensitive personal information, it must be ensured that the hospitals' information systems are properly maintained, and any vulnerabilities are identified and timely patched. In addition, since the hospital has the technical capability of generating data reports and exchanging them with third parties, the platform must ensure that proper cybersecurity and privacy

safeguards are in place in order to protect the integrity of the data and most importantly—patient safety. Consequently, the hospital decides to adopt the CUREX platform in order to address these issues immediately. In conjunction with optimal recommended safeguards, CUREX delivers targeted measures for raising the cyber hygiene of healthcare organizations through the recommendation of strategies and methodologies for training and raising awareness activities, targeted towards healthcare employees (administration, medical, and IT personnel) on cybersecurity and privacy risks incurred during data exchange. Training involves the development of cybersecurity defending skills, e.g., empowering social engineering defenses. In this way, healthcare employees will feel more confident in handling and exchanging sensitive data and improve their capabilities to perform their daily professional tasks effectively and in a secure fashion."

Generally, the use case approach scope presented in this work is always with respect POC systems cybersecurity and privacy management that help hospitals and care centers mitigate these risks, which becomes even more crucial when POCs' data needs to be exchanged within the different services of the hospital. Therefore, the use case does not explore the contents of the HIS system, but it manages the concepts of cybersecurity and privacy risk assessment. Together with trust, which is achieved with a shareable, verifiable, unmodifiable log in the blockchain; and cyber hygiene, which are the set of strategies and associated measures in the form of human-centric controls for raising cybersecurity and data privacy awareness of different employee groups in healthcare organizations. For this aim, three validation scenarios in the use case approach have been planned for assessing different cybersecurity and privacy situations of interest, and described in the following subsection.

Use Case Validation Scenarios

In this work three scenarios are defined as in [12] for the presented use case (and also accounting for misuse cases): "network configuration" where the use case scenario is not threatened by cybersecurity nor privacy risks, in order to perform an assessment in a normal operation of the use case; "outpatient appointment check" where the misuse case scenario is threatened by a denial-of-service attack, that prevents legitimate users from accessing internet services, including patient access to outpatient information; and "visualization of clinical information" where the misuse case scenario proposes and inside URL attack to retrieve clinical information, causing also a privacy risk. These three scenarios presented, focused on POC systems and dealing with cybersecurity and privacy risks in a healthcare, are depicted in Figure 2, and described below.

- Scenario 1: network configuration (POC)

In this scenario, no cybersecurity attack nor information privacy leakage is simulated, but still new configurations to the IT infrastructure are simulated. In particular, it is simulated that the IT department has been requested to re-arrange IT infrastructure of the hospital, including medical devices, due to a health crisis situation, as occurred in 2020 due to the COVID-19 pandemic. For such a request, the IP/MAC address links of the medical devices pointing the servers are modified. In this situation, CUREX platform detects that the IP/MAC address links have been modified but no cybersecurity nor privacy risk has occurred. Therefore, the overall combined cybersecurity and privacy risk score obtained through the CUREX platform should be low.

- Scenario 2: outpatient appointment check (smartphone app)

In this scenario, a distributed denial-of-service (DDOS) attack is simulated which is considered as high risk for cybersecurity and low risk for privacy. A participant is registered as a new simulated patient to access the simulated patient's information through the test smartphone app, but a DDOS attack happens resulting with the smartphone app functionality breaking down. Therefore, the participant is not able to access to the information due to an out-of-service notice. In this situation, the CUREX platform has

to provide a high score for cybersecurity risk, while a low privacy risk score, which both values combined results with the overall value of medium risk score reported by CUREX.

- Scenario 3: visualization of clinical information (HIS)

In this scenario, a URL hacking cybersecurity attack with leakage of privacy information is simulated. The simulated scenario is that a participant, simulating to be a medical doctor, wants to have access to a medical image and to a report of a simulated patient, but intentionally accesses another patient's data instead of the originally planned patient's data. Therefore, the simulated cybersecurity attack causes also a privacy leakage of information, implying that both the cybersecurity and privacy information risks scores of CUREX platform should be high.

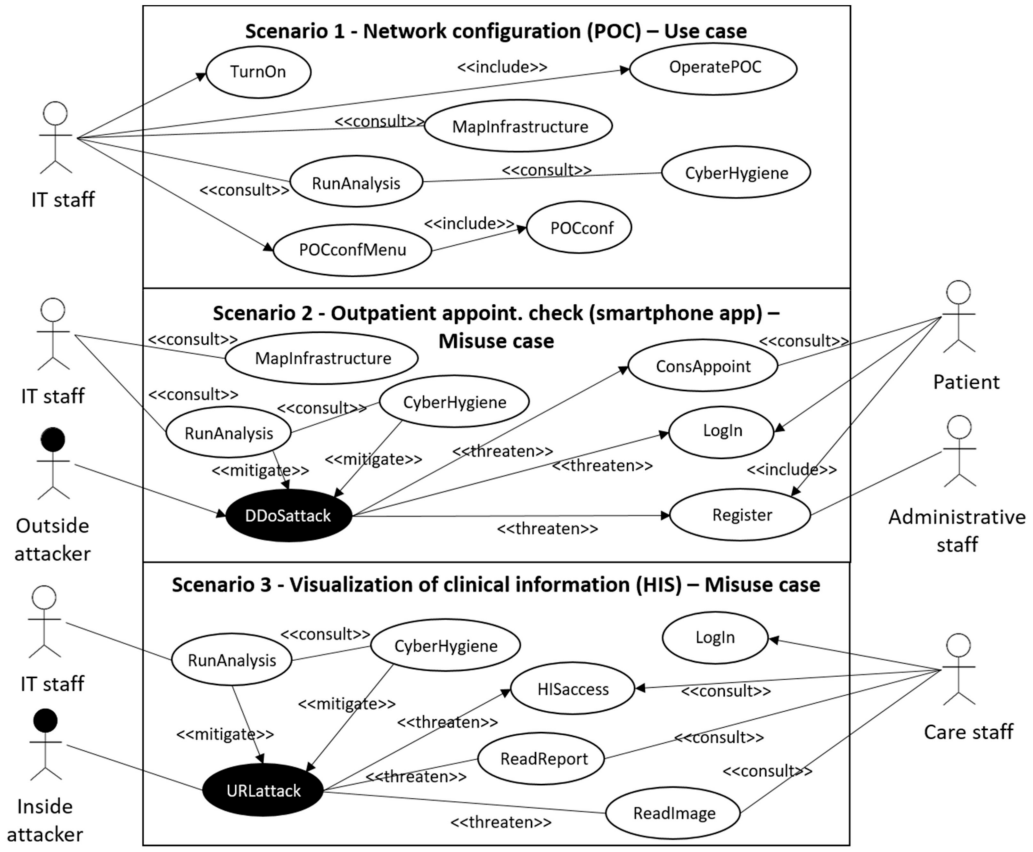

Figure 2. Diagram of the proposed use case described as in [12]. (**top**) Use case scenario diagram of the steps of the scenario for the communication of simulated clinical data with medical devices. (**middle**) Misuse case scenario diagram of steps of the scenario to access services through the smartphone app. (**bottom**) Misuse case scenario diagram of steps of the scenario to access to documents and images.

In particular, it is of high interest to at least pilot with Scenario 1 and either Scenario 2 or Scenario 3. Scenario 1 does not involve a cybersecurity attack but allows CUREX toolkit to compute the cybersecurity and privacy risk when no attacks are detected. For Scenario 1, results should provide low risks to the organization and therefore, they can continue sharing the data being requested. While the rationale behind Scenarios 2 and 3 involves simulating a cybersecurity attack and/or privacy leakage. The latter allows to assess the CUREX platform in terms of how scores change and analyze the quality of the suggested mitigation measures.

3. Develop Technical Infrastructure and CUREX Tools

The technical developments for the use case proposed is a recreation of part of the IT infrastructure of the hospital, also representative of many healthcare centers, in a pre-production environment. It is relevant that it is a parallel develop infrastructure since it is not possible to apply cybersecurity and privacy attacks and threats in a real infrastructure with real patient data and in-use equipment. Here resides one of the main points to apply use case approaches. In particular, as shown in Figure 3, the use case environment is firewall-disconnected, in any means of access, from the main infrastructure of the hospital. Therefore, the entire piloting environment is simulated but at the same time is highly representative of a real infrastructure. In particular, in Figure 3a, it is depicted the different entities composing the IT infrastructure develop together with elucidating its logical connections to the different components. Moreover, Figure 3b shows the logical arrangement of virtual local area networks (VLANs) that consistently sectorize the different entities through the firewall hardware device. Consisting of three VLANs: (i) for users to operate the workstations, (ii) for the POC medical devices, and (iii) the different servers and client applications to support the available services. Furthermore, the smartphone is connected to the use case environment through regular Wi-Fi or other internet access routes, but through a specific dedicated parallel connection channel to avoid any interference to the real infrastructure.

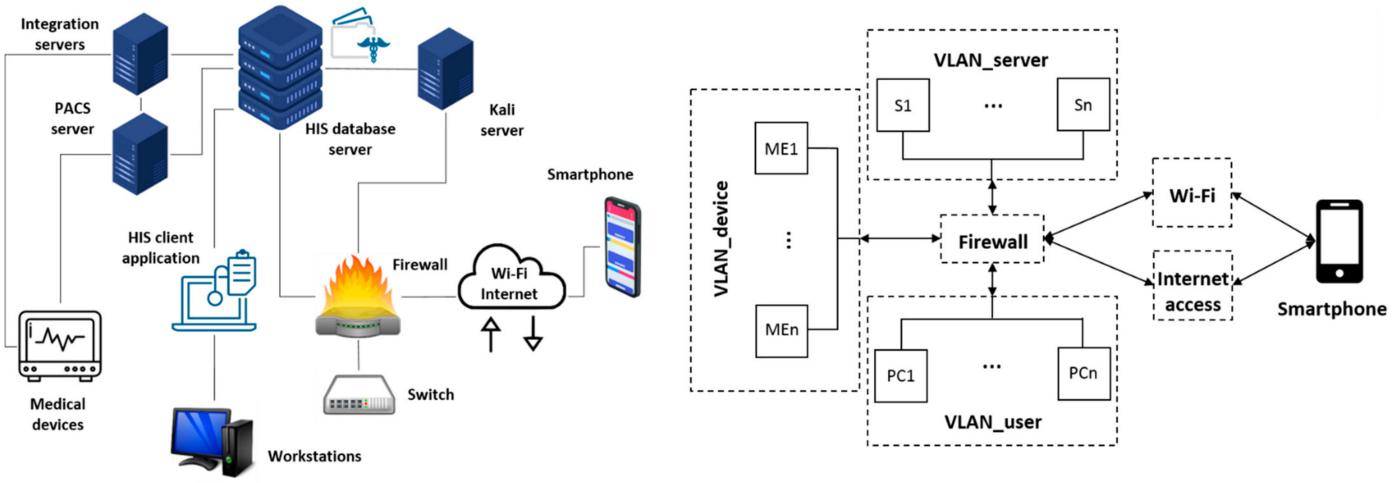

Figure 3. Logical infrastructure diagrams of the use case. (**a**) Components of the infrastructure and their connections. (**b**) VLANs sectorization for the workstations, POC medical devices and serves, all handled by the firewall, as well as for the smartphone.

In the created environment for the use case, the workstations or PCs run under Windows 10 operating system. The servers are placed in VMware machines and the medical devices have different versions of Windows, (e.g., Windows 7 and 10) and Linux distribution operating systems. The smartphone application to be assessed in the use case runs on a smartphone (android v9). Furthermore, several servers exist to have available integration engines, HIS, image server, and service integrators. In detail in Table 1, the following entities take part of the develop infrastructure.

Furthermore, the dedicated hardware for the use case is 8 vCPU and 48 GB RAM (servers and services installed in the infrastructure do not modify the indicated capacity values because they are accounted for aside of these values). The infrastructure is sized for 10 concurrent virtual private network (VPN) connections to allow different technical tool owners access to the use case infrastructure. Finally, different specific versions of operating systems are considered for the servers, working stations, virtual stations, smartphones, medical devices and emulators (Windows 7, Windows 10, Linux, etc.).

Table 1. Main components of the infrastructure and sectorization with VLANs.

Main Components	VLANs
HIS client application: either accessed from the CITRIX server farm or from a PC that has the client version installed locally, connects to the HIS database, which is installed in the hospital's data center (DC). Workstations: 4 PCs are placed inside VLAN user with the basic programs together with hospital's user credential handling procedures (credentials). HIS database server: consists of a cluster of servers that contains all the information stored. Kali Linux Server: Debian-based Linux distribution aimed at advanced penetration testing and security auditing. Firewall: The hospital's DC is generally supervised by a firewall system in which specific rules are programmed. VLAN user, VLAN server and VLAN device are connected bi-directionally to the firewall. Switch: Dedicated 20G LACP link to the cluster of servers and a 10G LACP link to the rest of the network's elements. PACS image server: Images are stored on a server called PACS (picture and archiving communications system). To retrieve the images, from the HIS, a call is made to a URL through a unique identifier of the patient's image study. Integration server: Used to collect all the data and external files and integrate them into HIS, either in the database or on the file server, or by external links using identifiers. Medical equipment: Two medical devices and an emulator are placed in VLAN_device. Medical devices can be real hardware or simulated/emulated software. Smartphone: Connection through Wi-Fi (open Wi-Fi validated via capture portal), using a specific identification that the firewall allows it to be visible and operating for this use case scenario; and/or using internet access (back-bone connection or mobile connection 3G/4G).	The firewall is configured to sectorize the use case in four virtual networks and controls the visibility of the three VLANs, the Wi-Fi and internet access to allow connecting the smartphone to the pre-production infrastructure. User, server and device VLANs are connected bi-directionally to the firewall. PCs in VLAN_user with the basic programs and user credential handling procedures. Servers in VLAN_server with: integration engines, HIS, image server, and service integrators. Medical devices in VLAN_device with real hardware preferably; otherwise simulated/emulated. Smartphone in Wi-Fi (open Wi-Fi validated via captive portal) with app test version installed.

Principally, the HIS is a replica of the original HIS (implemented with the collaboration of the normal provider of the HIS maintenance and development works) but with all information cleared and only simulated images, reports and information have been included, generated by the IT department. The networks details of the use case infrastructure are detailed in Table 2.

Table 2. Network details of mounted servers in the use case infrastructure, open virtual appliances (OVAs), configured VLANs and virtual workstations.

IP	Host	Notes	System	Domain	Name	IP/Port Number	
172.21.40.2	DEVCUREXSAVAC	HIS server CUREX	Centos 7.7, BBDD Oracle 11.2.0.4.0	40	CUREX_SERVER	172.21.40.0/24	
172.21.40.3	PREPACS	Preproduction PACS server CUREX	Windows 2016, IIS. Ports DICOM 1010, 1011 and 104	41	CUREX_USER	172.21.41.0/24	
172.21.40.4	PREPACSSQL	Preproduction PACS SQL server CUREX	Windows 2016, SQL Server	42	CUREX_ME	172.21.42.0/24	
172.21.40.5	DEVCUREXSAVI05	Integration HIS sever CUREX	Windows 2012, Apache Tomcat				
172.21.40.6	DEVCUREXSAVIFS	HIS Template server CUREX	Windows 2012, File server				
172.21.40.7	DEVCURESSAVIFS1	HIS Reports server CUREX	Windows 2012, File server	IP	Host	Mask	System
172.21.40.8	DEVCUREXXASVC01	Virtualisation server CUREX	Windows 2012R2 Citrix Server	172.21.41.2	pccurex01	255.255.255.0	Windows 10
172.21.40.9/24	DEVCUREXADT01	Asset Discovery server Curex_Server	OVA	172.21.41.3	pccurex02	255.255.255.0	Windows 10
172.21.41.5/24	DEVCUREXADT02	Asset Discovery server Curex_User	OVA	172.21.41.4	pccurex03	255.255.255.0	Windows 10

Notice that all IPs and ports' information is safe in terms of cybersecurity and information privacy because they are not used and isolated from the real hospital's infrastructure. Moreover, the operating systems of the workstations and PCs are selectable between Windows 7 and Windows 10, which are commonly used operating systems among health providers. Windows XP is no longer in use at the hospital facilities.

Lastly, in Table 3 is described the different information that has been created or generated considering the different POC systems in the IT infrastructure, together with the technical addressable information from the smartphone application.

Table 3. Description of the information sharing capacity, POC medical devices and smartphone within the use case developments.

Information Sharing Capacity	POC Medical Devices and Emulated Devices	Smartphone Addresable Information
Implemented 3 sectorizations (VLANs) of the IT infrastructure (managed by the general Firewall). Mounted and configured 8 servers. 3 working stations/PCs. Two hardware medical devices and one software emulator device. HIS mounted and capacity to generate simulated data in several formats (word documents, pdfs, etc.). Smartphone test application and server with access to the use case infrastructure.	Medical Device 1: Ultrasound Siemens Acuson Antares. Medical Device 2: Electrocardiogram RDPC Technic Assistance heart tablet. Emulated Medical Device 1: professional modality simulator (mounted in the infrastructure and configured). X-ray machine RAÏM modality simulator.	When the smartphone is connected to the infrastructure: the connection is via Wi-Fi (or other internet access proxies). It is relevant to monitor the app server, and less relevant the app terminal itself. The app server is configured to support a test app. The app server is a regular server, but also configured for the test app for the use case. The app server provides simulated data to the SAVAC_CUREX (HIS).

In particular, Medical Devices 1 and 2 are not updated for clinical practice, but they operate correctly and are valid for the demonstrations. The emulated Medical Device 1 is based on protocol DICOM (Digital Imaging and Communication in Medicine) and it is an image viewer for biomedical imaging that was developed by the Biomedical Digital Imaging Center of UDIAT-CD S.A [22]. This emulator was developed with Java technology and can therefore be used in almost any computer and graphic operative system. Finally, the different available information from the POC systems allows to assess the cybersecurity and privacy risk at different levels in the develop use case infrastructure, which as described below, will be captured, processed and analyzed by the different CUREX platform technical tools.

CUREX Platform Solution

The CUREX solution analyzes information coming from the monitoring infrastructure to compute cybersecurity and privacy risk scores associated to the data exchange in a health domain. CUREX has five discrete areas: (i) asset and vulnerability discovery, whose goal is to discover the system's assets and any information related to their associated vulnerabilities; (ii) threat intelligence, aiming at detecting real time abnormal behaviors on users, and devices, as well as anomalies in the data in order to identify new and unknown threats; (iii) risk management, aiming at producing risk scores and optimal safeguards towards a cyber-strategy of the healthcare organization; (iv) trust enhancing, which will make use of a decentralized platform based on blockchain technology to store and share private and sensitive data, as described in [17,18]. Particularly, the interactions between the different tools of CUREX are depicted in Figure 4.

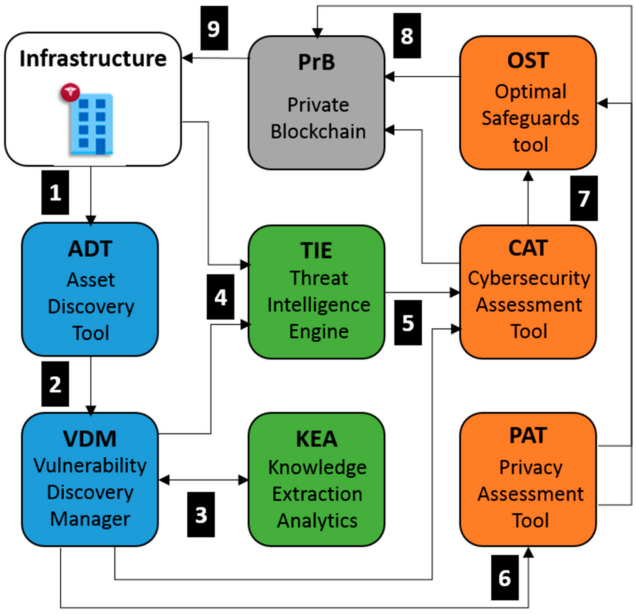

Figure 4. Interaction between CUREX's tools with regards the infrastructure where they have been deployed.

An example considering Scenario 3, defined in Section 2, CUREX platform's enumerated actions are defined in the following ordered list below, once the CUREX solution has been deployed in the infrastructure:

1. ADT scans the infrastructure and identifies the entities and resources that have direct connection with the HIS [18]. A list of assets (including IP addresses, open ports, services and/or operating systems running in each asset) is generated by the ADT and shared accordingly with other CUREX tools. It is worth noting that for this particular scenario, the ADT has discovered that some workstations are running outdated versions of the operating system (OS).
2. Upon reception of the asset list, VDM performs a vulnerability scanning, using as input the list of IP addresses discovered by the ADT. As a result, VDM generates a report containing a list of security vulnerabilities associated to all the hospital's resources (assets) detected in the network's hospital infrastructure [23]. In particular, the VDM report contains a list of critical exploitable vulnerabilities against the outdated OS, and it is initially shared with KEA for further analysis.
3. Upon reception of the vulnerability report, KEA performs a machine learning analysis using the log events generated in the infrastructure in order to detect new threat patterns that could potentially harm the system [24]. New threat patterns are added to the VDM, which enriches the vulnerability report to be shared with other CUREX tools.
4. TIE receives the enriched vulnerability report by the VDM and in parallel, receives logs from events originated in the end-user's infrastructure. In particular, TIE employs anomaly detection and analytics to detect intrusion and malicious activities using a variety of tools and techniques. As a result, TIE is able to generate correlated alarms indicating potential threat incidents detected in the monitored infrastructure. The generated alarms are then shared with other CUREX tools for further processing and analysis. In this example, a URL-attack is detected against one of the resources, which can potentially give uncontemplated access to the HIS database. The generated alarms are then shared with other CUREX tools for further processing and analysis.
5. CAT receives a list of vulnerabilities from the VDM, and a list of events and alarms from TIE, which along with the risk pattern models and configuration configured by the infrastructure IT managers, provides the required input to perform a cybersecurity analysis. As a result, global and individual scores are generated, making it possible to identify critical events to assign priorities for their treatment. For each score, a set

of mitigation measures is proposed by CAT. The generated CAT scores are stored in the PrB, and the list of mitigation measures is shared with OST [20] for its analysis and optimization. Regarded the considered example, one of the provided mitigations provided in the generated list and selected by the IT user could be "map inputs values to actual filenames/URLs, etc., and reject all other inputs", which is highly efficient and with medium associated cost of implementation.

6. In parallel, PAT also receives the vulnerability report from VDM and performs a privacy risk assessment of the organization and the platform by evaluating GDPR compliance [25]. Similar to CAT, a set of mitigation measures is proposed by PAT [26]. The generated PAT scores are stored in the PrB, and the list of mitigation measures is shared with OST for its analysis and optimization.
7. OST receives in real time the CAT and PAT mitigation measures and performs an optimal safeguard analysis based on values of costs and efficacy provided by the end-user. As a result, the OST displays in its dashboard the list of mitigation measures ranked by priority. This output is also stored in the PrB.
8. PrB receives on the one hand the CAT and PAT scores, and on the other hand, the mitigation measures from OST. CAT and PAT qualitative scores are merged, and a unified risk score is generated.
9. After the optimal mitigation measures are applied to the systems and their infrastructure by the IT end-user, a new scan from the ADT will be performed and the process restart from Step 1 to finally end with the CAT and/or PAT results that will decrease accordingly during the new risk assessment.

For all three scenarios, defined in the previous section, CUREX should provide cyber hygiene recommendations and procedures to improve the capabilities and training of participants with respect to cybersecurity and privacy risks.

4. Pilot Plan and Validation Test Steps

The proposed use case allows testing and evaluating cybersecurity and privacy risks, as well as for the CUREX platform potential impact on data exchange in healthcare services, focused on modelling and analyzing POC systems. First, a pilot plan has been defined in Table 4, in order to define the overall specificities involved with the use case. Notice that the defined pilot plan can be used as the base model to define other use cases in the current context as well as in other use case models.

Table 4. Use case pilot plan definition.

Item	Description
Involved Partners	The use case pilot is executed involving participants at the hospital facilities. It is convenient for the execution of the pilot because the participants will use computers enabled to run the steps of the defined validations on the develop infrastructure. Furthermore, the preamble presentations and interview/focus groups are hosted as well at the piloting premises with the involvement of the participants and use case managers.
Participants	IT staff. It is the group composed of professionals belonging to the IT department of the hospital. They have experience with the technical aspects of the HIS, medical devices and cybersecurity. Assistance staff. It is the group composed of medical doctors and nurses, who may belong to different medical specialties. These professionals have knowledge and experience in consulting clinical information in the HIS. Administrative outpatient staff. It is the group composed of professionals belonging to the hospital outpatient administrative staff. These professionals have knowledge and regularly plan the appointments for the patients of the hospital.

Table 4. *Cont.*

Item	Description
Short Description	The hospital IT department has raised concerns about the cybersecurity issues that may emerge from the operation and the communication of the clinical data. Indeed, since the data contains highly sensitive personal information, it must be ensured that the hospitals' information systems are properly maintained, and any vulnerabilities are identified and timely patched. In addition, since the hospital has the technical capability of generating data reports and exchanging them with third parties, the platform must ensure that proper cybersecurity and privacy safeguards are in place in order to protect the integrity of the data and—most importantly—the patient safety. Consequently, the hospital decides to adopt the CUREX platform in order to address these issues immediately. In conjunction with optimal recommended safeguards, CUREX will deliver targeted measures for raising the cyber hygiene of healthcare organizations through the recommendation of strategies and methodologies for training and raising awareness activities, targeted towards healthcare employees (administration, medical, and IT personnel) on cybersecurity and privacy risks incurred during data exchange. Training will involve the development of cybersecurity defending skills, e.g., empowering social engineering de-fences. In this way, healthcare employees will feel more confident in handling and ex-changing sensitive data and improve their capabilities to perform their daily professional tasks effectively and in a secure fashion.
Timeline	The pilot execution will consist of two phases, following the Agile Flow Review methodology, in order to provide feedback to the tool owners and means of validation. Enough participants are involved in the pilots to collect sufficient result in order to generate relevant outcomes. Therefore, more than one session with different participants is executed. In general, each session will last 4 h, consisting of the preamble presentation, running the relevant scenarios of the pilot and conducting the interviews/focus group. Given that three working stations are available in the mounted infrastructure, each session can consist of six participants covering the three different types described above. Around four sessions in the timeframe of the first phase of the pilot can be executed. Depending on the outcome of the first stage of the pilot, the second phase of the pilot can be arranged as explained before, or adjustments of the planning can be arranged.
Preconditions	The CUREX framework has modelled, monitored and assessed the HIS infrastructure. As a result, the CUREX framework is able to provide assessment scores and give a proper set of cybersecurity and privacy recommendations to the hospital in the form of reports and manuals dictating possible best practices to correct issues identified in the infrastructure. Furthermore, the involved CUREX tools have been properly configured.
Preamble	A preamble PowerPoint presentation will be given and explained to each participant for them to better understand the use case and CUREX solution in general.

Furthermore, following the use case diagram defined in Section 2, the different validation actions of the three different scenarios have been detailed step-by-step in Table 5. Generally, the three scenarios have a common "start point" step. In this so-called STEP 0, the system is analyzed by CUREX tools providing some recommendations about cybersecurity and privacy risks. Once they are implemented, it is continued with each on-demand scenario. Lastly, the execution of the different scenarios provides cyber hygiene recommendations.

Table 5. Use case scenarios validation steps-by-step plan description.

Step #	Description of Tasks	Step to Execute	Expected Results
Scenario 1—Network Configuration (POC)—Use Case Scenario			
1	Turn on medical devices and emulators	IT participant presses turn-on buttons of the two medical devices and initiate the emulator	Medical devices and emulator operating
2	Mapping of original IT infrastructure	IT participant executes CUREX ADT tool	Map the IT infrastructure with servers and devices present
3	Operating medical devices and emulator	IT participant capture information for the two medical devices and display CT image from emulator	Confirmation of the proper operation of the medical devices and emulator

Table 5. *Cont.*

Step #	Description of Tasks	Step to Execute	Expected Results
Scenario 1—Network Configuration (POC)—Use Case Scenario			
4	Access to medical device configuration section	IT participant operates the configuration menu of one of the medical devices (with user and password)	Access (possible risk of default password)
5	Modify the network configuration data and modify roles and permissions on the firewall	IT participant introduces new IP address link for the medical device and the firewall	Modified original emitter details for the medical device and firewall
6	Mapping of updated IT infrastructure	IT participant executes CUREX ADT tool	CUREX detect different correlation between IP and MAC address
7	Operating medical devices and emulator	IT participant captures information for the two medical devices and display CT image from emulator	Confirmation of the proper operation of the medical devices and emulator
8	Execution of CUREX platform	IT participant runs CUREX analysis and annotates score from the CVT. Both IT participant and participant perform the feasible recommendations if needed	Score should be low, then participant performs the feasible recommendations given by CUREX to improve the resilience on cyber-security, privacy and cyber hygiene on the items related to this Test
Scenario 2—Outpatient Appointment Check (Smartphone App)—Misuse Case Scenario			
1	Mapping of original IT infrastructure	IT participant executes CUREX ADT tool	Map the IT infrastructure with servers and devices present
2	Simulate registering at front desk (private part of the test app)	IT participants creates and stores new user and credentials in the test app	Simulated administrative staff provides credentials
3	Participant logs in with new credentials	User participant opens app using the mobile phone and log in with PIN	Access to the private/confidential section of the test app
4	Participant consults the pending appointments	User participant clicks on the appointments section of the app	Webservice is launched and receives response of the appointments listed in the HIS
5	The test app is turned off (simulating DoS attack)	IT participant turns down the app test configuration (potentially it can be simulated with Kali Linux server as a DoS attack)	No petitions are served
6	Mapping of original IT infrastructure	IT participant executes CUREX ADT tool	Map of the IT infrastructure with servers and devices present
7	Participants checks the detailed information of a specific appointment	User participant click on a specific appointment	Out-of-service message is received
8	Execution of CUREX platform	IT participant runs CUREX analysis and annotates score from the CVT. Both IT participant and user participant perform the feasible recommendations if needed	Score should be medium, then participant performs the feasible recommendations given by CUREX to re-establish the score to low and to improve the resilience on cyber-security, privacy and cyber hygiene on the items related to this test
Scenario 3—Visualization of Clinical Information (HIS)—Misuse Case Scenario			
1	Login to Windows sessions	User participant introduces credentials	Log in against active directory.
2	Login to CITRIX	User participant validates that the credential displayed in CITRIX are the same as Windows	Credential pass-through to CITRIX that will present the icons of those applications that the user has configured

Table 5. *Cont.*

Step #	Description of Tasks	Step to Execute	Expected Results
Scenario 3—Visualization of Clinical Information (HIS)—Misuse Case Scenario			
3	Login to HIS	User participant clicks on HIS client icon and introduce credentials	Access to HIS
4	Access to clinical history	User participant searches and clicks on "Visión Global" of the specific simulated patient	Structured data of HIS
5	Selection of report	User participant clicks on specific simulated report "informat"	Access to report
6	Selection radiological procedure (image)	User participant clicks on specific simulated CT image "RX button"	Open image in an external DICOM viewer through URL call, with a specific identifying unique number
7	Capture of image URL before pop-up Windows auto-closes (minimum and only security protection)	User participant clicks on specific simulated CT image "RX button" and copies the url from the web browser	Capture of the url call
8	Open web browser and manipulate iteratively the URL (simulating URL hacking attack)	User participant captures the url for the image call in the web browser and changes the last number of the line (potentially done automatically with Kali Linux server with a man-in-the-middle attack)	Access to different images
9	Execution of CUREX platform	IT participant runs CUREX analysis and annotates score from the CVT. Both IT participant and user participant perform the feasible recommendations if needed	Score should be high, then IT participant implements the feasible recommendations given by CUREX to re-establish the score to low and to improve the resilience on cyber-security, privacy and cyber hygiene on the items related to this test

Particularly, each scenario is composed of a limited number of steps in an ordered sequence (Column 1), with clear indications of the performed action (Column 2), description of the step to perform (Column 3) and the outcome, which might be linked to a specific requirement assessment, produced by each step (Column 4). Hence, the step-by-step validation test plan described above provides sufficient information for the different participants to execute the actions required for each scenario of the use case. However, also the test plan also allows the use case session managers to monitor the execution of the scenario as well as to annotate any relevant information to be further analyzed afterwards. In this way, the use case specific test plans serve as case report forms for each scenario, as described in the following section.

5. Discussion on Risk Assessment Capability

There are numerous use case approaches in the literature to model cybersecurity and privacy requirements [27]: multilateral, unified modeling language (UML)-based, goal-oriented, problem frame-based, risk/threat analysis-based, and common criteria-based approaches. In particular, the use case approach proposed in this work is based on misuse cases extending UML diagrams and relies on a form of risk/threat analysis to capture various cybersecurity and privacy risks, to elicit threat scenarios in a structured form. Furthermore, it provides mitigation recommendations relaying on CUREX solution, or accordingly, directions given by other cybersecurity and information privacy risk assessment solutions. Therefore, the dimension of assessment capability attained in the proposed use case is large, where a list of contemplated requirements allowed to be assessed are shown in Table 6.

Table 6. List of contemplated assessable cybersecurity and privacy requirements.

Cybersecurity and Privacy Requirements	Priority/Domain	Description
Securing integrity information regarding risk assessment and interactions with the infrastructure	Mandatory/Cybersecurity	The complete monitoring and assessment flow must be reflected in the private blockchain contents providing support for the fact that end components can connect and disconnect without prior notice.
Check credentials match from previous steps	Optional/Cybersecurity	Credentials must be passed between steps, from the medical staff, which informs them on the system, to the SAVAC system. Each step must get and pass the credentials through the next step. The CUREX system should monitor, as an important part of its risk assessment phase whether these holds.
Verify/check that registration number and patient ID are not correlated	Optional/Privacy	The patient must provide a valid identification number to the medical staff in order to search for his/her history. The system needs a way to correlate the patient history number with a European unique patient history number.
Database and communication channel assessment	Mandatory/Cybersecurity	Data must travel safely between database and front-end HIS application. Communication network must ensure no data sniffing or data loss, and no third party can change the data between the database and the front-end. Patient data is involved.
Assessments/safeguards regarding prevention of URL headers from being hacked	Optional/Cybersecurity and Privacy	Application headers are formatted text that can be modified. If this occurs, an attacker could see image from another patient and/or the image can be saved in another patient record history.
Cyber hygiene level of target groups	Mandatory/Cybersecurity and Privacy	Targeting different groups (e.g., care staff, IT staff, administrative staff) cyber hygiene strategies should increase awareness on cyber security and the new GDPR.
User friendly interface of tools and applications	Mandatory/Cybersecurity and Privacy	Targets digital infrastructures, but is meant to be operated to a significant extent by non-IT experts.

The requirements listed in Table 6 are not particular to the CUREX solution but general to other cybersecurity and information privacy risk assessment solutions, contemplating both functional and non-functional requirements, and they can be enlarged following best-practice guidelines, privacy-by-design methodologies and IT standards [28]. Furthermore, the described requirements in Table 6 encompass some mandatory as well as optional requirements, regarding cybersecurity and privacy risks. Mandatory level is considered when the requirement is a must, without which the described functionality cannot be provided. However, optional level is assigned when the requirement is only recommended to have an appropriate performance of the tool/service. The assigned level of mandatory requirements has been qualitatively weighted and agreed between different stakeholders (software developers, healthcare providers, and researchers) within the CUREX consortium. Where the qualitative weighting has been assigned by mapping the requirements' urgency by the end-users to the performance goals elicited by the technical development of the specific CUREX tools. Moreover, the requirements' considerations detailed in our use case, in some part, are highly valid since they are also considered in other information risk analysis works as [4,29–32]. Hence, the methodology followed can be applied to other use cases and risk assessment solutions [33,34].

Regarding the employed assessment scoring tools, it is first described the automated cybersecurity and information privacy risks solution proposed for the use case using CUREX platform, but also other assessment procedures will be discussed. In particular, in the proposed use case, the cybersecurity assessment is based in employing state-of-the-art machine-learning algorithms and technologies combined into an automated solution for hospitals and health care centers to understand inherent risks that emerge from exchanging health data and drive the decisions towards successfully mitigating the risks [23]. However, the information privacy risks are assessed based on the OLISTIC Enterprise risk management suites (ERMS) [26]. Where, finally, to calculate the overall impact to all data assets of the healthcare organization it integrates NIST's guide for security risk assessment [35]. Nevertheless, other cybersecurity and information privacy risk assessment approaches are available such as the common vulnerability scoring system (CVSS) [36,37]. In particular, CVSS assigns severity scores (based on a formula that depends on several metrics that approximate ease of exploit and the impact) to vulnerabilities, allowing the prioritization of actions and resources according to the threats.

In this direction, in the detailed step-by-step use case's scenarios of Section 4, each requirement to be assessed is introduced at a specific position of the steps to be performed by the participants. This helps tracing the requirements along the validation test plan to ensure that the full scope of the requirements is assessed. Moreover, following an hybrid Agile-predictive methodology [38], the use case manager can decide to add or delete requirements to be assessed in the different scenarios. In addition, in this way, participants can provide specific feedback during the demonstration, validations and evaluation of the use case through questionnaires, focus groups and interviews. Nevertheless, the planning of the experimental protocols involves the consideration of ethical [28], legal aspects [25], data usage and data processing [39], testing recruitment and informed consent, as well as the impact of each use case and the roadmap [40]. Hence, a first validation round can be conducted to gather the participant's results and reports to provide feedback for improving or updating the requirements in order to improve the functionality of the tools and platform solution, according to the end-user needs, beliefs and requirements.

Importantly, usability feedback depends heavily on the subjective perceptions and the prioritization of needs of each user [41]. Therefore, it is appropriately to carry out the use case with the sufficient number of participants to co-create and to ground solutions that fit the final users. This is because healthcare IT decision-makers will not adopt an IT-health related technology if it does not fulfil their current levels of need, such as security and safety, no matter how simple to use, innovative, affordable or powerful the technology is [42].

Furthermore, the use case proposed also places emphasis on improving cyber hygiene through the recommendation of strategies and methodologies for training and raising awareness activities for a healthcare institution's personnel. Its validation focuses on the highly challenging condition of POC systems; spanning medical devices, big data clinical history and smartphones (and can potentially assess other Internet-of-things devices) through the three appropriately selected use case's scenarios. Furthermore, the focus of the described scenarios has been placed on insider threats, hence easily our use case approach allows to develop new scenarios with other very relevant threats to healthcare, as ransomware attacks, which has proven to have had a high occurrence and a large impact in the past. In particular, one could think of a scenario where the data stored in the HIS system is encrypted (e.g., by the WannaCry ransomware attack) using medical devices with legacy operating systems as entry points triggered by a participant's misstep (which could be mounted combining Scenarios 1 and 3). Lastly, the proposed use case could be extended with security scenarios (mitigation measures) together with derivation of business continuity considerations and cost-effectiveness of the mitigation measurements.

6. Conclusions

This work describes a particular use case to assess cybersecurity and privacy risks for POC systems, but it can be readily generalized to other common related risk situations in healthcare. In particular, the proposed use case has been focused on allowing to experiment with the cybersecurity and privacy risk assessment for POC systems in a relevant healthcare IT infrastructure. Hence, the work presented is ambitious not only concerning the considerations regarding IT solution architectures, but also in different domains and number of requirements that are included in the use case to be assessed. Moreover, the particular use case considerations regarding the CUREX platform can be generalized to other solution platforms and use cases, following the indications provided in the discussion section.

Furthermore, it has been argued that developing a use case approach is crucial to improve the user experience and increase user adoption. In this regard, the designed and develop IT infrastructure contain a HIS system, actual servers, POC systems and portable devices (e.g., smartphone). Such a development is the base to allow running different oriented scenarios for the participation of different stakeholders and end-users. Particularizing the configurations to conduct threat scenarios (misuse cases), as well as the regular functionality scenarios.

Moreover, the three develop specific use case scenarios, for cybersecurity and privacy risk assessment, have relevant differences on the outcomes in several dimensions as well as in the adversary profiles. Furthermore, an extra scenario regarding highly recurrent and impactful ransomware attacks has been raised at the end of the discussion section. Although the ransomware attack has not been fully developed, the described use case approach in this work holds promise as highly moldable tool to assess the cybersecurity and privacy risk of other threats of interest. Finally, we have also contemplated and included in the different scenarios the demonstration steps for a cybersecurity and privacy trust-enhancing platform in development (CUREX), which is part of an international research and innovation effort lead by academics, companies and healthcare providers.

In addition, cybersecurity and privacy protection are expanding with more laws and regulations expected to be issued in the coming years. Therefore, it is important for healthcare providers to continue monitoring and adopting successful developments, demonstrated in validated use cases, complying with the prescribed security and privacy protection requirements, and be aware of the applicable risks and exposures; especially for POC systems in IT health infrastructures. Thus, despite the increasing levels of government attention on information technology risks in healthcare and increased funding, we still need to define critical use cases, as the one proposed in this work, that can deliver the biggest impact in healthcare through cybersecurity and privacy risk assessments, to ensure the highest quality for what is actually being delivered on the ground or showing promise in terms of developments in the pipeline.

Author Contributions: Conceptualization M.J. and D.N.-L.; methodology J.M.Z. and G.G.-G.; Software R.A., J.P. and R.R.; writing—original draft M.J.; validation D.N.-L., R.A., J.P., J.M.Z., G.G.-G. and R.R.; writing—review and editing D.N.-L. and R.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 826404.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Written informed consent is required from the participant(s) in the planned pilots.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would also like to thank all the CUREX consortium members for their work: UPRC, ATOS, ALRS, CLS, INTRA, S5, LEX, 8BELLS, UBI, SURREY, UPM, UCY, AUTH, SERMAS, FPHAG and KI.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jalali, M.S.; Kaiser, J.P. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *J. Med. Internet Res.* **2018**, *20*, e10059. [CrossRef] [PubMed]
2. Jofre, M. Holistic View of Healthcare Cybersecurity Ecosystem; Research Gate GmbH: 2020. Available online: https://www.researchgate.net/publication/343722649_Holistic_View_Of_Healthcare_Cybersecurity_Ecosystem (accessed on 21 July 2021).
3. Tulasidas, S.; Mackay, R.; Hudson, C.; Balachandran, W. Security Framework for Managing Data Security within Point of Care Tests. *J. Softw. Eng. Appl.* **2017**, *10*, 2. [CrossRef]
4. Williams, P.A.; Woodward, A.J. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Med. Devices* **2015**, *8*, 305–316. [CrossRef] [PubMed]
5. Reason, J. Human error: Models and management. *BMJ* **2000**, *320*, 768–770. [CrossRef] [PubMed]
6. Sardi, A.; Rizzi, A.; Sorano, E.; Guerrieri, A. Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability* **2020**, *12*, 7002. [CrossRef]
7. Wagner, I.; Boiten, E. Privacy Risk Assessment: From Art to Science, by Metrics. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*; Springer: Cham, Switzerland, 2018; pp. 225–241. [CrossRef]
8. Hameed, S.S.; Hassan, W.H.; Latiff, L.A.; Ghabban, F. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Comput. Sci.* **2021**, *7*, e414. [CrossRef] [PubMed]
9. Coronado, A.J.; Wong, T.L. Healthcare Cybersecurity Risk Management: Keys to an Effective Plan. *Biomed. Instrum. Technol.* **2014**, *48*, 26–30. [CrossRef] [PubMed]
10. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
11. Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development, Third Edition [Book]. Available online: https://www.oreilly.com/library/view/applying-uml-and/0131489062/ (accessed on 26 April 2021).
12. Sindre, G.; Opdahl, A.L. Eliciting security requirements with misuse cases. *Requir. Eng.* **2005**, *10*, 34–44. [CrossRef]
13. Cockburn, A. *Writing Effective Use Cases*, 3rd ed.; Addison-Weley: Reading, MA, USA, 2001.
14. Constantine, L.L.; Lockwood, L.A.D. *Software for Use: A Practical Guide to the Models and Methods of Usage-Centered Design*, 1st ed.; Addison-Wesley: Reading, MA, USA, 1999; Available online: https://www.oreilly.com/library/view/software-for-use/9780768685305/ (accessed on 26 April 2021).
15. Jacobson, I.; Christerson, M. *Object-Oriented Software Engineering: A Use Case Driven Approach*, 1st ed.; Addison-Weley: Reading, MA, USA, 1992.
16. Yue, T.; Briand, L.C.; Labiche, Y. Facilitating the transition from use case models to analysis models: Approach and experiments. *ACM Trans. Softw. Eng. Methodol.* **2013**, *22*, 1–5:38. [CrossRef]
17. CUREX | Secure and Private Health Data Exchange. Available online: https://curex-project.eu/ (accessed on 26 April 2021).
18. Diaz-Honrubia, A.J.; Gonzalez, A.R.; Zamorano, J.M.; Jiménez, J.R.; Gonzalez-Granadillo, G.; Diaz, R.; Konidi, M.; Papachristou, P.; Nifakos, S.; Kougka, G.; et al. An Overview of the CUREX Platform. In Proceedings of the 2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS), Cordoba, Spain, 5–7 June 2019; pp. 162–167. [CrossRef]
19. Mohammadi, F.; Panou, A.; Ntantogian, C.; Karapistoli, E.; Panaousis, E.; Xenakis, C. CUREX: seCUre and pRivate hEalth data eXchange. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence-Companion Volume, New York, NY, USA, 14 October 2019; pp. 263–268. [CrossRef]
20. Panda, S.; Panaousis, E.; Loukas, G.; Laoudias, C. Optimizing Investments in Cyber Hygiene for Protecting Healthcare Users. January 2020. Available online: http://arxiv.org/abs/2001.03782 (accessed on 15 March 2021).
21. Jofre, M. Minimum Quality Standard for Cybersecurity Training in Healthcare–SecureHospitals.eu; ResearchGate. 2020. Available online: https://www.researchgate.net/publication/343722644_Minimum_quality_standard_for_cybersecurity_training_in_healthcare_-_SecureHospitalseu (accessed on 21 July 2021).
22. Fernàndez-Bayó, J.; Barbero, O.; Rubies, C.; Sentís, M.; Donoso, L. Distributing Medical Images with Internet Technologies: A DICOM Web Server and a DICOM Java Viewer. *Radiographics* **2000**, *20*, 581–590. [CrossRef] [PubMed]
23. Gonzalez-Granadillo, G.; Diaz, R.; Veroni, E. *A Multi-Factor Assessment Mechanism to Define Priorities on Vulnerabilities Affecting Healthcare Organizations*; ITASEC 2021; p. 13. Available online: http://cgi.di.uoa.gr/~{}xenakis/Published/93-A%20Multi-factor%20Assessment%20Mechanism%20to%20Define%20Priorities%20on%20Vulnerabilities%20affecting%20Healthcare%20Organizations/VDM-CameraReady.pdf (accessed on 26 April 2021).
24. Bellas, C.; Naskos, A.; Kougka, G.; Vlahavas, G.; Gounaris, A.; Vakali, A.; Papadopoulos, A.; Biliri, E.; Bountouni, N.; Granadillo, G.G. A Methodology for Runtime Detection and Extraction of Threat Patterns. *SN Comput. Sci.* **2020**, *1*, 238. [CrossRef]
25. Data Protection. European Commission-European Commission. Available online: https://ec.europa.eu/info/law/law-topic/data-protection_en (accessed on 16 May 2021).
26. Papamartzivanos, D.; Menesidou, S.A.; Gouvas, P.; Giannetsos, T. A Perfect Match: Converging and Automating Privacy and Security Impact Assessment On-the-Fly. *Future Internet* **2021**, *13*, 30. [CrossRef]
27. Mai, P.X.; Goknil, A.; Shar, L.K.; Pastore, F.; Briand, L.C.; Shaame, S. Modeling Security and Privacy Requirements: A Use Case-Driven Approach. *Inf. Softw. Technol.* **2018**, *100*, 165–182. [CrossRef]

28. Boeckl, K.; Fagan, M.; Fisher, W.; Lefkovitz, N.; Megas, K.N.; Nadeau, E.; O'Rourke, D.G.; Piccarreta, B.; Scarfone, K. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*; NIST IR 8228; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019. [CrossRef]
29. Lin, T.-W.; Hsu, C.-L. FAIDM for Medical Privacy Protection in 5G Telemedicine Systems. *Appl. Sci.* **2021**, *11*, 1155. [CrossRef]
30. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Chapter One-Blockchain Technology Use Cases in Healthcare. In *Advances in Computers*; Raj, P., Deka, G.C., Eds.; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41. [CrossRef]
31. McFarland, R.J.; Olatunbosun, S.B. *An Exploratory Study on the Use of Internet_of_Medical_Things (IoMT) in the Healthcare Industry and Their Associated Cybersecurity Risks*; ICOMP'19 2019; p. 7. Available online: https://www.proquest.com/openview/c3d186a57f9cae20d87d6f5d5f9f92a9/1?pq-origsite=gscholar&cbl=1976348 (accessed on 20 July 2021).
32. Wang, L.; Jones, R. Big Data, Cybersecurity, and Challenges in Healthcare. In Proceedings of the 2019 SoutheastCon, Huntsville, AL, USA, 11–14 April 2019; pp. 1–6. [CrossRef]
33. Grguric, A.; Khan, O.; Ortega-Gil, A.; Markakis, E.K.; Pozdniakov, K.; Kloukinas, C.; Medrano-Gil, A.M.; Gaeta, E.; Fico, G.; Koloutsou, K. Reference Architectures, Platforms, and Pilots for European Smart and Healthy Living—Analysis and Comparison. *Electronics* **2021**, *10*, 1616. [CrossRef]
34. Anastasopoulou, K.; Mari, P.; Magkanaraki, A.; Spanakis, E.G.; Merialdo, M.; Sakkalis, V.; Magalini, S. Public and private healthcare organisations: A socio-technical model for identifying cybersecurity aspects. In Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, New York, NY, USA, 23 September 2020; pp. 168–175. [CrossRef]
35. Joint Task Force Transformation Initiative. *Guide for Conducting Risk Assessments. National Institute of Standards and Technology*; NIST Special Publication (SP) 800-30 Rev. 1; NIST Special Publication: Gaithersburg, MD, USA, 2012. [CrossRef]
36. Yannis, N. D3.3 Vulnerability Assessment as a Service v1. WP3—Cyber Security Risk Assessment & Beyond—Sphinx Intelligence. SPHINX Consortium. 2019. Available online: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5d0ebe11a&appId=PPGMS (accessed on 16 July 2021).
37. Common Vulnerability Scoring System. Wikipedia. 21 June 2021. Available online: https://en.wikipedia.org/w/index.php?title=Common_Vulnerability_Scoring_System&oldid=1029633418 (accessed on 17 July 2021).
38. Agile Practice Guide | Project Management Institute. Available online: https://www.pmi.org/pmbok-guide-standards/practice-guides/agile (accessed on 17 May 2021).
39. Azarm-Daigle, M.; Kuziemsky, C.; Peyton, L. A Review of Cross Organizational Healthcare Data Sharing. *Procedia Comput. Sci.* **2015**, *63*, 425–432. [CrossRef]
40. Vanclay, F. International Principles for Social Impact Assessment. *Impact Assess. Proj. Apprais.* **2003**, *21*, 5–12. [CrossRef]
41. Petrie, H.; Bevan, N. *The Evaluation of Accessibility, Usability, and User Experience*; Stepanidis, C., Ed.; CRC Press: Boca Raton, FL, USA, 2009. [CrossRef]
42. Alrahbi, D.; Khan, M.; Hussain, M. Exploring the motivators of technology adoption in healthcare. *Int. J. Healthc. Manag.* **2021**, *14*, 50–63. [CrossRef]