IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 November 2023, accepted 27 November 2023, date of publication 30 November 2023,
date of current version 12 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3338170

RESEARCH ARTICLE

A Comprehensive Model for Securing Sensitive Patient Data in a Clinical Scenario

**ANTONIO LÓPEZ MARTÍNEZ, MANUEL GIL PÉREZ,
AND ANTONIO RUIZ-MARTÍNEZ, (Senior Member, IEEE)**
Department of Information and Communications Engineering, University of Murcia, 30100 Murcia, Spain

Corresponding author: Antonio López Martínez (antonio.lopez41@um.es)

This work has been partially funded by the strategic project Development of Professionals and Researchers in Cybersecurity, Cyberdefense and Data Science (CDL-TALENTUM) from the Spanish National Institute of Cybersecurity (INCIBE) and by the Recovery, Transformation and Resilience Plan, Next Generation EU.

ABSTRACT The clinical environment is one of the most important sources of sensitive patient data in healthcare. These data have attracted cybercriminals who pursue the theft of this information for personal gain. Therefore, protecting these data is a critical issue. This paper focuses on an analysis of the clinical environment, presents its general ecosystem and stakeholders, and inspects the main protocols implemented between the clinical components from a security and privacy perspective. Additionally, this article defines a complete use case to describe the typical workflow within a clinical setting: the life cycle of a patient sample. Moreover, we present and categorize crucial clinical information and divide it into two sensitivity levels: High and Very Sensitive, while considering the severe risks of cybercriminal access. The threat model for the use case has also been identified, in conjunction with the use case's security and privacy needs. This work served us as basis to develop the minimum security and privacy requirements to protect the use case. Accordingly, we have defined protection mechanisms for each sensitivity level with the enabling technologies needed to satisfy each requirement. Finally, the main challenges and future steps for the use case are presented.

INDEX TERMS Clinical scenario, patient data, privacy, security, threat model.

I. INTRODUCTION

The clinical setting is a significant part of the healthcare domain, involved in the process of diagnosing and treating patients. Essentially, the term "clinical" is often accompanied (i) by "laboratory", understood as the place where patient's samples are analyzed to diagnose injuries or problems; or (ii) by "data", referring to the data generated through the procedures conducted in the laboratory. This domain is one of the largest sources of data in the health sector [1] and has become more important in recent years because of the sensitivity of the information generated there [2], which is associated with physical persons.

Clinical data is of particular interest to cybercriminals because it contains sensitive information about patients that is also long-lived, unlike another type of information, e.g., credit cards, which can be suspended after notification to the bank [3]. With this information, cybercriminals can defraud insurers, create fake treatments, and impersonate real people. The impersonation or theft of information is known as a *Data breach* and is one of the greatest threats to the clinical scenario and healthcare. In 2022, several data breaches were produced with negative consequences, such as i) the Shields Healthcare Group data breach, where two million records (Medical Records, Patient IDs, etc.) with sensitive information were stolen; ii) the Broward Health data breach, where 1.3 million records were taken from the database; and iii) the Morley Companies data breach, where nearly half a million records were encrypted due to a ransomware attack [4]. In addition, cyberattacks could affect the health of patients through implanted devices used for their treatments, such as defibrillators and insulin pumps. Battery leakage and eavesdropping are two of the most common attacks on these types of devices [5].

In many cases, the clinical environment is also composed of old machines, which were created when security was not so

The associate editor coordinating the review of this manuscript and approving it for publication was Mehedi Masud.

important. Besides, these machines use proprietary software, which is complicated to analyze and protect. Therefore, there is a real need to protect the clinical domain as it is one of the primary information sources for healthcare since this is where patient samples are analyzed and treatments are applied. However, the origin of the attacks (insecure operations or security and privacy issues) is an important aspect to address. In this context, the work presented in [6] clarified this question. They analyzed the cyberattacks in Asian Organizations, which might be useful to have a clear picture. They found that the lack of anti-malware, poor infrastructure, lack of cybersecurity awareness among the healthcare staff, and the absence of risk management led to breaches in the healthcare sector. Besides, they found a survey by a US organization indicating that 60 percent of healthcare staff cited email as the main point of attack for compromising the system. This last aspect belongs directly to an insecure operation, in conjunction with efficient anti-phishing email detectors. Still, it is very important to analyze the clinical infrastructure and communications since deficiencies in this domain can support these insecure operations.

In this context, this paper aims to provide a complete view of the clinical environment, showing the general architecture with the stakeholders and components involved as well as the protocols used in the clinical area, and revealing the grade of security and privacy implemented by each one. It also presents the use case modeled in this article, the life cycle of a patient sample, defining the steps and their security and privacy needs. This paper also presents a specific threat model, including attacks that affect the use case defined. Moreover, this paper examines the possible types of clinical data generated and their uses in this sector, dividing them into two levels, depending on each data/use's sensitivity grade. This classification aims to present a list of protection mechanisms for each level, depending on an enumeration of requirements created for satisfying the security and privacy needs previously identified. All these novel contributions are defined to support future research works in the clinical domain.

The rest of the article is organized as follows. Section II explores the related works available in the literature, as well as the official standards and regulations. Section III presents the clinical environment and the definition of the use case with the clinical sample life cycle model. Section IV declares the threat model identified for the use case. Next, Section V develops the security and privacy requirements applied to the use case defined, with the minimum protection mechanisms identified for each of them. Finally, Section VI explains the conclusion and work's next steps.

II. RELATED WORK

This section shows a list of relevant papers found in the literature regarding the healthcare and clinical environment and the official mandatory regulations to be considered regarding security, privacy, and the protection of data in the healthcare and clinical sector.

A. REVIEW OF LITERATURE

In this section, we revise different articles that deal with the security and privacy requirements, needs, and technologies to use in the clinical domain. Table 1 compares the features used in the study of the works identified in the literature with this article to identify the contributions made. This table includes different columns regarding the content of each research work: work reference, the creation year, the domain (clinical or healthcare), review of clinical protocols, presentation of clinical or healthcare architecture, definition of the pathway or information flow produced in a clinical use case (as the one presented in Section III-C), classification of clinical data types, security requirements, secure technologies, secure mechanisms, inclusion of privacy in the work, and the presentation of a threat model for the use case.

The literature has widely examined security and privacy in healthcare in general. In this context, some reviews inspect security and privacy, current work in the field, and future steps in healthcare. To begin with, *Newaz* et al. [7] presented the security and privacy requirements of the healthcare environment, the threats (Denial of Service, Ransomware, etc.), and protection solutions (Side-channel analysis, hardware-based, software-based, etc.) focused on healthcare devices and applications, and the future research areas, such as the lack of standard communication protocols and privacy-preserving healthcare systems.

López et al. [15] complemented the previous work adding more security and privacy requirements, listing all threats that occurred in healthcare (Eavesdropping, Data breach, etc.) and aligned them with MITRE ATT&CK framework [17], classifying protection mechanisms researched in the literature (Blockchain-based, Anomaly detection, Proxy-based, etc.).

These articles are focused on healthcare from a generic point of view, in contrast to the work presented in this article, which deals with a more specific scenario, namely the clinical environment. The security aspects found in these works will be used to formalize the use case defined in Section III.

Regarding clinical environment-based works, *Cowan* [8] conducted research about security and confidentiality in laboratory computer systems. This work is the first found in the literature to talk about security in a clinical domain. The author presented different security guidelines for protecting a laboratory system, such as backing up data, safeguarding sensitive information, selecting good passwords, etc. He also defined the need for different security levels to provide granular access to laboratory records. Although it is an old paper, it is still interesting to introduce the clinical environment. *Ameen and Ahmed* [9] designed an e-laboratory system. They studied the main threats and protection mechanisms for this system (intrusion detection, network monitoring, etc.). *Kenimer* [11] addressed privacy in clinical laboratory science. She mainly studied the impact of laboratory information on patient safety, as well as the definition of a clinical decision support system. She evaluated the consistency of such a system in terms of privacy.

TABLE 1. Summary of the state-of-the-art studies revised (where Req. = requirements, tech. = technologies and mech. = mechanisms).

Ref.	Year	Field	Protocols	Use case			Security			Privacy	Threat Model
				Architecture	Pathway	Data Types	Req.	Tech.	Mech.		
[8]	2005	Clinical	-	-	-	-	-	-	✓	✓	-
[9]	2013	Clinical	-	-	-	-	-	✓	✓	✓	✓
[10]	2013	Clinical	-	-	-	-	✓	✓	✓	✓	-
[11]	2014	Clinical	-	-	-	-	-	-	-	✓	-
[12]	2019	Clinical	-	-	✓	-	-	-	-	✓	-
[7]	2021	Healthcare	-	✓	-	-	✓	✓	✓	✓	✓
[13]	2022	Clinical	-	-	✓	-	-	-	-	✓	-
[14]	2022	IoT	-	-	-	-	-	✓	✓	✓	-
[15]	2023	Healthcare	-	✓	-	-	✓	✓	✓	✓	✓
[16]	2023	Clinical	-	-	-	-	-	✓	✓	✓	✓
Ours	2023	Clinical	✓	✓	✓	✓	✓	✓	✓	✓	✓

Cucoranu et al. [10] explained Protected Health Information (PHI) as patient data that must be protected. The authors showed protection mechanisms that can be implemented in a pathology laboratory: (i) Hardware security to protect the physical facilities (Endpoint security); (ii) Software security to protect the software components (Passwords, Single Sign-On, Access control, Biometrics, and Audit trails); (iii) Data security to protect the data itself (Data integrity, Data protection, Data recovery, and Data encryption); (iv) Internet security (Firewall and Antivirus); (v) Interfaced instruments (analyzers) with an external connection; and (vi) Mobile devices mainly from practitioners. This work was performed in 2013 but gives readers a clear view of laboratory security and privacy aspects to be considered.

Patel et al. [16] addressed the cybersecurity in a clinical environment. They identified the main components of this scenario, such as Electronic Medical Record systems (EMR) and middleware, which will be presented in Section III. They listed Malware, Phishing, Man-in-the-Middle, and Insider Threats as relevant attacks in this environment. Besides, they showed different security controls, such as establishing a cybersecurity culture, using strong passwords, encrypting data, etc., all of them from a high-level perspective. Finally, they enumerated interesting regulatory and standard groups like the Health Insurance Portability and Accountability Act (HIPAA) and the National Institute of Standards and Technology (NIST) to identify the security and privacy requirements for the health domain. These are the most interesting papers regarding security and privacy in a clinical environment found in the literature.

To continue, the works conducted in [12], [13] presented two pathway models about two use cases in the clinical environment: osteosarcoma diagnosis and medical imaging care. These pathway models present the workflow followed by the patient data and samples in the two use cases defined. They are very useful to understand the clinical environment, and both will be used in Section III to define the clinical sample life cycle pathway model, the use case defined in this article. In addition, both works exposed security and privacy elements. *Rahmouni* et al. [12] designed some security labels to protect sensitive data (Anonymized, Encrypted, Obfuscated, etc.), while *Essefi* et al. [13] defined a model to enforce sensitive data protection. However, both works do not cover the security and privacy field from a selection mechanism perspective to protect this environment. The work conducted by *Yang* et al. [14] presented the Internet of Things (IoT) as a new tendency in the recent context. This work is not directly related to the clinical domain, but the laboratories also have IoT, and the future laboratories could need technologies like the one presented by *Yang* et al.. They implemented a federated learning (a machine learning technique to train algorithms in a distributed manner) solution to apply with IoT technology.

To conclude, the relevant papers studied in this area still present some gaps that are addressed in this article. Table 3 graphically exposes all these gaps. To cope with them, this article contains the following contributions: (i) explanation of the main architecture and components involved in a clinical domain as well as the definition of a complete use case with these components; (ii) review of the main clinical protocols from a security and privacy perspective; (iii) classification of the different clinical data types, explaining the grade of sensitivity of all of them; (iv) enumeration of a threat model with the attacks targeted in the clinical environment; (v) definition of the security and privacy requirements to secure the clinical use case; and (vi) presentation of technologies to effectively protect the use case regarding the sensitive data involved in each requirement.

B. OFFICIAL REGULATIONS

The official regulations provide the vision that international governments have about protecting healthcare. In this context, the European Union (EU) and the United States (US) are two principal regions working on legislation to regulate and manage this critical environment. The clinical environment is included as a subset of healthcare. Therefore, it is also affected by the directives created for healthcare.

Starting with the US, HIPAA is the official regulation for processing and protecting data in the health environment [18]. HIPAA implements the HIPAA Security Rule to safeguard PHI and the HIPAA Privacy Rule to address the use of people's health information.

The Food and Drug Administration (FDA) [19] is a regulatory agency of the US Department of Health and

Human Services. This agency enforces regulations and standards to protect food, drugs, etc. Its most relevant part is the Medical Device regulation because it ensures that medical devices meet safety and performance standards and monitors their manufacturing, distribution, and use. The NIST [20] is another US agency focused on promoting innovation and industrial competitiveness by advancing measurement science, standards, and technology. It has efforts in the health domain, providing biomedical research, guidelines to secure Electronic Health Records (EHR), and cybersecurity standards, in general, which may support the creation and development of new protection mechanisms.

EU has also designed different regulations. The most important is the General Data Protection Regulation (GDPR) [21], created for the management and protection of European citizen data. GDPR defines Personal Data being the information that directly or indirectly identifies an individual. It includes laws for different purposes, such as data processing, individual rights, user consent, data security and breach notification, data transfers, and data protection impact assessments. Regarding data, an interesting EU regulation appears with the Data Governance Act [22], where the highly sensitive category of health data is addressed. This regulation is focused on establishing a framework for data sharing and data intermediaries within the EU. This regulation is interesting since it addresses the highly sensitive category of health data, which will be used in this article in Section III-D, especially in transferring this information to third countries.

Finally, the European Health Data Space (EHDS) [23] regulation implements a European framework where citizens from different countries can attend any hospital in the European continent and receive medical assistance. The regulation presents the requirements needed to implement this framework. It will be considered in the following sections when presenting the classification of health data. In the work performed in [24], a questionnaire was designed to identify possible recommendations to apply to the EHDS. Some interesting recommendations obtained were the adoption of cybersecurity standards, expanding open infrastructures, and facilitating secondary use of health data for research and innovation. This type of use for health data will be deeply addressed in Section III-D.

All regulations directly impact the implementation of security and privacy in healthcare and, subsequently, the clinical environment. These regulations have been considered in the contributions performed in this article, making them regulations-compliant. For instance, the contribution presented in Section III-D complies with the content shown in the EHDS regulation.

III. USE CASE: CLINICAL SAMPLE LIFE CYCLE PATHWAY MODEL

This section presents the components involved in a clinical environment, the protocols used, and their limitations in terms of security and privacy. Besides, this section defines the clinical sample life cycle pathway model, the use case defined in the context of this work.

A. BACKGROUND

The clinical environment is composed of different components, as observed in Figure 1. This representation of the clinical environment has been validated with a national company that installs laboratory machines in Spanish hospitals, including the reference University Clinic Hospital of the authors' geographical zone.

The components are usually assigned to a hospital, which houses laboratories and external components. On the one hand, the Electronic Medical Record (EMR) system and the Laboratory Information System (LIS) are deployed in the hospital scope since the information they contain is shared between all hospital stakeholders. The EMR is the central component that stores the patient's EHR and implements the different procedures to perform in a healthcare environment (prescriptions, telemedicine, patient portal, etc.). The LIS connects the laboratory instruments (analyzers) and the EMR. This component understands the data format of the result generated by the analyzer and uploads it to the EMR registry.

On the other hand, the Middleware elements and the analyzers are placed in the laboratory scope as the final machines in charge of analyzing the patient samples (understood by the Middleware as tests). The Middleware component deployed in each computer can be linked to one or more analyzers to collect and process the result of the tests received and send the results to the LIS for further analysis and validation. The analyzers are responsible for generating the results of physical samples collected from patients. All these components are communicated by different clinical protocols, which are presented in the following section.

B. CLINICAL PROTOCOLS

Figure 1 shows different protocols which are used by the components presented above. These protocols have been extracted from the literature [25], [26] and from interviews made with the Spanish clinical company about the clinical domain. Moreover, these protocols are analyzed from a security and privacy perspective and following their position in the OSI layers. As a result of this analysis, we can point out that the clinical protocols do not implement effective security and privacy mechanisms to protect clinical data. Besides, we might highlight the date of creation of these protocols, which still is quite old. The summary of protocols studied is presented in Table 2, where the year of creation, the purpose, the mapped OSI layer to allocate it, and whether the protocol presents security/privacy mechanisms and threats are encompassed.

In the analyzer/Middleware scope, LIS1-A (ASTM E1381) [27] and LIS2-A2 (ASTM E1381) [28], designed by the American Society of Testing and Materials (ASTM), model the communication. The former specifies the low-level protocol to transfer messages between laboratory instruments

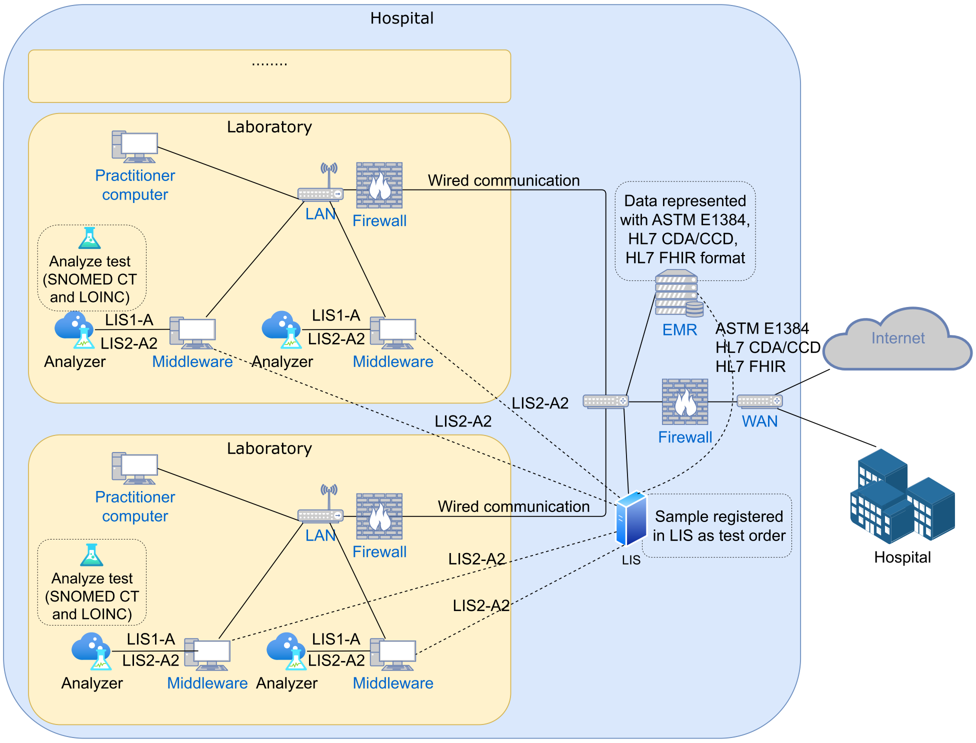

FIGURE 1. **Clinical environment ecosystem.**

and computer systems, while the latter defines the information transmitted over LIS1-A standard. LIS2-A2 is also used between Middleware and LIS to send the information collected from the analyzers. From a security perspective, LIS1-A does not implement any data security [29]. Regarding LIS2-A2, it includes demographic information (patient address, telephone number, etc.), which is not protected and might be breached by a malicious actor. The last standard from the ASTM organization is ASTM E1384 [30], which defines the EHR structure and content. In security and privacy terms, it includes operational principles in its content related to security and privacy, such as confidentiality protection, type of information, practitioner signature, etc.

Health Level Seven (HL7) is a family of standards to define clinical data exchange. In this context, HL7 v2 is considered one of the most widely implemented standards in healthcare information systems [31]. It describes the data shared between healthcare providers and clinical scenarios. This standard delegates the security to lower OSI layers being vulnerable to different attacks, such as Denial of Service and Flooding attacks [32].

HL7 v3 Reference Information Model (RIM) improves HL7 messaging format using object paradigm, which is formalised using Unified Modelling Language (UML) diagrams [33]. Compared with HL7 v2 in security and privacy terms, HL7 v3 also fails to implement specific mechanisms to secure the data transmitted with it [34]. Other HL7 standards are HL7 v3 Clinical Document Architecture (CDA) and Continuity of Care Document (CCD). HL7 CDA is an XML-based standard that allows interoperability between healthcare providers and patients. It defines the structure and semantics of a ‘‘clinical document’’ encompassing all information related to medical reports. HL7 CCD is a collaboration between ASTM and HL7 also to provide interoperability. Essentially, HL7 CCD is a subset of HL7 CDA with the combination of ASTM's Continuity of Care Records. This standard intends to give an understanding of a patient care event at a particular time [35]. In security terms, both HL7 CDA and CCD do not incorporate any protection mechanisms for the data modeled [36].

The last HL7 standard is HL7 Fast Healthcare Interoperability Resources (FHIR), which implements a modular approach by exposing health data entities as services using HTTP-based REST and API [37]. These entities are formalised as FHIR Resources, managed with the API, and exposed to stakeholders as web services. HL7 FHIR offers security recommendations in different areas, such as authentication, access control, etc. [38]. Besides, it implements security labels to model aspects like the confidentiality of the data [39]. However, this protocol is susceptible to threats like replay and man-in-the-middle (MitM) attacks (several intermediates), horizontal scalability (if the server is compromised), etc. [40].

Regarding medical digital imaging, Digital Imaging and Communications in Medicine (DICOM) is used by the typical clinical machines that generate medical images,

TABLE 2. Protocols available in the clinical scenario.

Protocol	Year	Purpose	OSI layer	Security/Privacy	
				Protection Mechanisms	Attacks and Weaknesses
LIS1-A/ASTM E1381	2002	Low-level protocol to transfer the information from clinical laboratory instruments (analyzers) to computer systems (Middlewares)	1-2	—	Health Data Exposure Risk
LIS2-A2/ASTM E1394	2004	Establishes the information transmitted between laboratory instruments and computer systems over LIS1-A protocol	1-2	—	Data breach, Data Exposure
ASTM E1384	1996	At the data level, it defines the format of Electronic Health Records (EHR)	7	Security and privacy-related content	Application-layer attacks (Web-based, Storing-based, etc.)
HL7 v2	1990	Defines the information transmitted between healthcare providers and clinical scenarios	7	—	DoS and Flooding attacks.
HL7 v3 RIM	1997	Incorporates UML diagrams and implements semantic representation of clinical data to achieve interoperability	7	—	DoS and Flooding attacks.
HL7 v3 CDA	2000	Implements "clinical documents" definition to exchange information between healthcare providers and patients	7	—	Application-layer attacks
HL7 v3 CCD	2007	ASTM-HL7 collaboration to define patient care events	7	—	Application-layer attacks
HL7 FHIR	2014	Implements a modular approach based on HTTP REST and API and creates FHIR resources to define health data entities	7	Security and privacy labels	MitM attack, replay attack, horizontal scalability
SNOMED CT	2002	Defines a clinical reference terminology to represent clinical information	7	—	—
DICOM	1993	Establishes the format of medical imaging and related information	7	—	Remote attacks, fuzzing attacks
LOINC	1994	Represents the values obtained from the clinical laboratory instruments to their human interpretation	7	—	—

such as X-ray machines, Ultrasound machines, etc. [41] Communication security is not addressed in its definition, which has produced different threats with devices using this standard; for example, remote attacks on heart pacemakers, Bluetooth defibrillators, etc. [42]. Besides, complex attacks can be performed as the work addressed in [43], where they demonstrated a DICOM vulnerability based on Fuzzing technology.

Finally, SNOMED CT and Logical Observation Identifiers Names and Codes (LOINC) are presented. SNOMED CT is a comprehensive and multilingual clinical reference terminology representing clinical information. It is understood as an ontology of medical concepts. LOINC is a community-built universal code that allows the exchange of laboratory and clinical observations [44]. For both SNOMED CT and LOINC, there is no security/privacy-related content in the literature since these standards are only used to identify the clinical data and laboratory results and the form of measuring them.

C. CLINICAL SAMPLE LIFE CYCLE PATHWAY

The two previous sections have offered a complete view of the stakeholders/components as well as protocols in the clinical domain. In this section, a complete use case is presented to cover the lack of an effective model in the clinical environment.

Figure 2 presents the sample life cycle pathway model, showing the life cycle of a patient's sample, from the medical appointment until the procurement of the final result. This model has been inspired by the works performed in [12], [13], presented in Section II-A. Besides, the model presents the threats affecting each use case process. This threat model will be detailed in Section IV.

The pathway starts with the patient's request to make an appointment (*step 1*), which is sent to the EMR, authenticating the patient (*step 2*) and establishing the doctor-patient appointment. This is the traditional form of making an appointment, but some exceptions might appear here, such as accidents where the patient is brought to the emergency department by ambulance. Such cases do not fall under this generic use case.

Next, the practitioner requests access (*step 3.1*) to the patient's data (medical history, patient information, etc.) on the precise date. If the patient is not registered, a new entry is created in the EMR (*step 3.2*). Otherwise, the doctor retrieves the essential data for the consultation (*step 3.3* and *step 4*). In this procedure, the model supposes that the patient has authorized the doctor to access his/her medical data. At this time, the practitioner generates an order (*step 5*) to start the collection of samples through a Computerized Physician Order Entry (CPOE) [45].

The CPOE is registered into the patient EHR (*step 7*) according to ASTM E1384, HL7 CDA/CCD, or HL7 FHIR standards, which contains the patient's medical history and clinical data. Furthermore, the test is established into the LIS (*step 6*), part of the laboratory environment, through HL7 standards format (HL7 v2 and v3). This component comprises a collection of software, operating systems, and hardware designed to serve the operational processes of the clinical scenario [25]. Essentially, the LIS contains one or more dictionary tables for each operation process. Afterward, the practitioner (e.g., nurse) takes the sample (*step 8*) collected from the patient, adds a bar-code, and sends it to the LIS (*step 9.1*).

The LIS completes the entry created (*step 9.2*) above with the following information: demographic information that samples can have from the patient, a specimen number that links the test order and patient information, and if the sample contains different containers; each one receives a Container ID (CID), all being modeled with SNOMED CT and LOINC standards. This CID is the ID that the practitioner visualizes in the instruments when the sample is examined. Besides, the LIS can receive information from the doctor-patient appointment, which is used in the next steps for completing billing information. For public institutions, the billing model would be circumvented.

The Middleware receives the requests from the LIS to start an analysis (*step 10*), communicating it with the analyzer

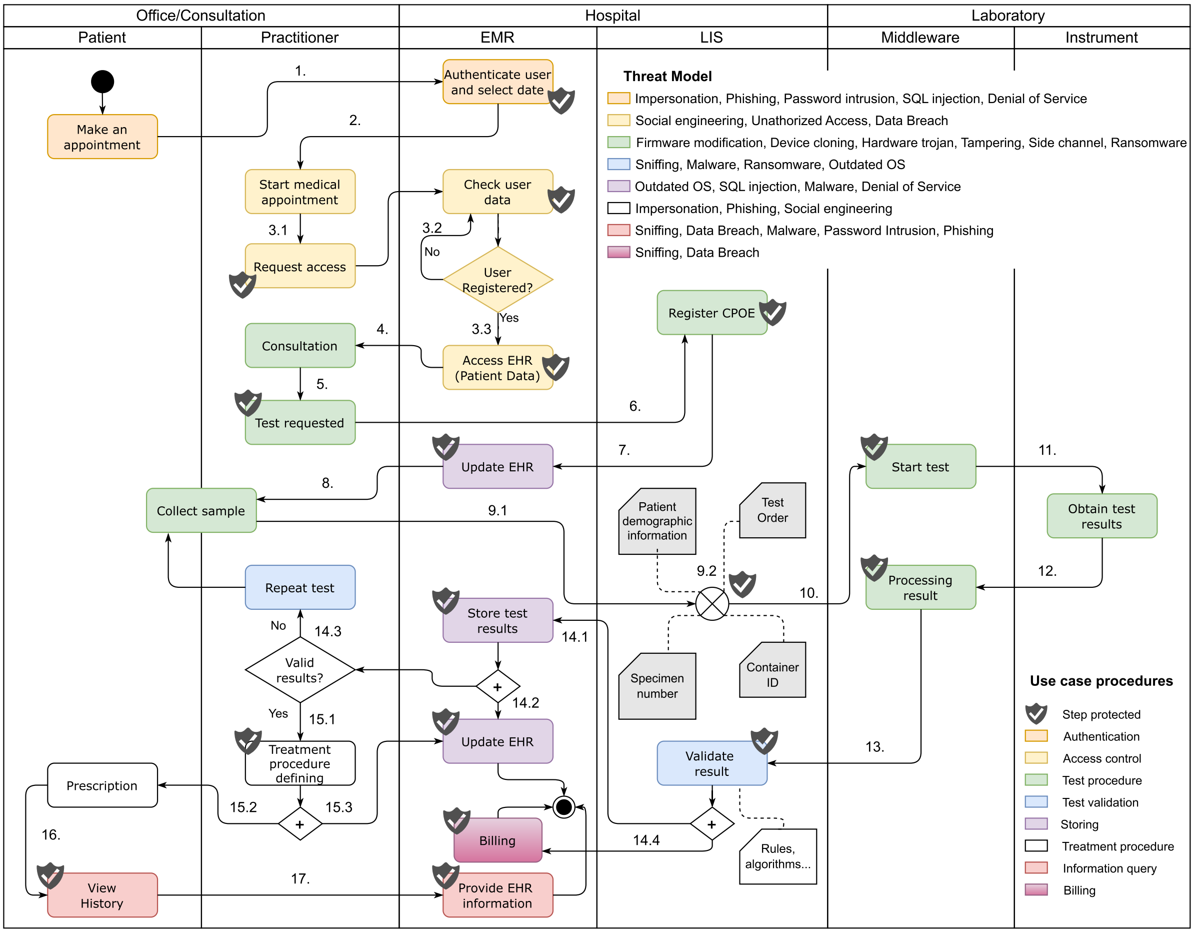

FIGURE 2. Clinical sample life cycle pathway model.

through ASTM standards (LIS1-A, LIS2-A2), and obtaining the result (from the analyzer) to perform the first processing with rules and mechanisms pre-configured by the vendor. Furthermore, the analyzer vendor provides Medical Device Interface (MDI) software to allow communication between the LIS and the analyzer. Thus, the LIS receives the results and understands the format and the content provided.

The analyzer examines the sample (*step 11*) and the result is collected by the Middleware (*step 12*), processed in the first instance, and sent to the LIS (*step 13*). At this stage, the LIS verifies the results through different algorithms and rules installed in this component. These algorithms/rules can be customized, such as a validation to inspect biochemical data of cancer patients [46]. This procedure can conclude in an invalid result, updating the EHR patient (*step 14.1* and *step 14.2*), and starting the procedure established, such as restarting the sample collection process (*step 14.3*). Besides, the billing component of EMR is informed (*step 14.4*) with the operation details and information about the test (process performed with the patient sample) analyzed by the LIS in order to apply the necessary expenses. In a correct validation, the doctor-patient communication is produced anew via a physical appointment (*step 15.1*), a call, etc. In this encounter, the procedure is defined for the patient's disease/problem (*step 15.2* and *step 15.3*).

Finally, both the user and practitioner must have access to the EHR to retrieve the patient's history (steps 16 and 17), such as tests and treatment procedures produced. Thanks to this register, it is possible to have control of the patient data, used in the future to know the patient pathologies, allergies, etc. As detailed, the black point found in the bottom part of the diagram is the final state of the workflow, reached from various steps.

As an individual procedure, the LIS and the EMR systems store information (steps 7 and 14.2) about the patient and the test performed to conduct doctor treatment procedures. However, in some instances, secondary uses of data can appear to cover other needs in the clinical environment. They can be clinical uses (aggregated data to infer population outbreaks), operational uses (performance of analyzers), research uses (use data for designing new medications), business uses (calculation of costs), etc. [25]. Illustrated by these secondary uses, a consistent data warehousing must be designed, taking in mind aspects like clinical data standards, the performance requirements of the requests, and so on.

D. CLASSIFICATION OF CLINICAL AND HEALTH DATA

In the clinical environment, primary and secondary uses for the clinical data can appear, understood the former as the data needed for the health services affecting and maintaining the state of health of people, and the latter as the data needed for the clinical uses, operational uses, research uses, business uses, etc.

This section has the purpose of classifying the different types of clinical and health data, taking into account these two families of uses.

This effort also supposes the division of health data uses into a classification, High and Very Sensitive, defined by the level of criticality of the specific information if a breach/attack is produced and the information is publicly exposed. First of all, the clinical and health data uses are extracted from the EHDS [23], regulation commented in Section II-B. EHDS presents a complete list of primary and secondary uses of health data. The classification in High and Very Sensitive levels is realised by exploring the Data Governance Act [22], which defines the specific data uses that are very sensitive, especially when shared with third countries.

Here, the contribution of the paper at hand is classifying such primary and secondary uses of health data extracted into the two levels commented. The data uses allocated in the primary use are directly used in the treatment procedure defining and maintaining people's health. In this case, all types are allocated to the Very Sensitive level of security and privacy protection due to this information's criticality. On the other hand, the types of secondary uses encompass a wider variety of uses. In this case, it is possible to classify uses into the High and Very Sensitive levels, depending on the purpose of the information. The decision and validation to include several secondary uses in the Very Sensitive level are derived from the EHDS regulation, which takes the Data Governance Act regulation to affirm such secondary uses as highly sensitive, as commented above.

In Table 3, starting with the first level, *Data impacting on health* incorporates data affecting health without having personal data from a social, environmental, and behavioural perspective. *Pathogen genomic data* includes information about possible pathogens affecting human health, i.e., studies, results, and conclusions. *Identification data related to practitioners* contains information about the professionals involved in treating patients. *Feedback from data holders* regarding data permits, understood as the decision of a health data provider to a data user for processing the electronic data specified in the data permit. *Health-related administrative data* includes the information stored from claims, reimbursements, bureaucracy, etc. *Population-wide health data registries* encompass grouped data from data holders to derive information to the population level. *Questionnaires and surveys* collect people's wellness concerning services offered by practitioners, physical facilities of the hospital, etc. Finally, *Electronic Health Data (EHD) related to education, lifestyle, and wellness* can store various information related to wellness people, from insurance to education and lifestyle data.

Regarding the Very Sensitive level of secondary use in Table 3, *Electronic Health Records (EHR)* imply all patient information, with their history, treatments, laboratory results, etc. This information can be used, for instance, in aggregated studies to obtain possible information about pandemics. *Person generated health data* unites all health information belonging to a person, collected from medical devices (invasive, non-invasive), health apps, etc. *Human genetic, genomic, and proteomic data* collects the intrinsic human characteristics that everyone has from birth, such as his/her blood group. *EHD from medical registries for diseases* can require information from patients with certain diseases, which could be helpful in studies of other diseases. *EHD from clinical trials* is the information stored from the experiments performed to bring to market a new medicament or treatment. *EHD from medical devices* encompass the collection of information from these devices, as in previous use, but dedicated to creating or researching medicinal products and devices. To conclude, *EHD from biobanks and databases* are also used in the investigation in the clinical and biomedicine environment.

E. IDENTIFICATION OF SECURITY AND PRIVACY NEEDS IN THE USE CASE

Focusing on security and privacy, the whole process from Figure 2 should be secured, and selected components must implement protection mechanisms to secure user information. This section's contribution is composed of identifying the critical components/steps and presenting the current security mechanisms implemented by default in the pathway.

The EMR system, the LIS, and the Middleware must be protected with sophisticated security mechanisms. However, other elements can appear, such as networked drives hosted on servers administrated by the laboratory, hospital, external partners, etc., to implement, for instance, the data warehousing explained above. These elements are configured in a client/server networking and might store critical patient and sample data for primary and secondary uses offered as shared resources for different users.

On the other hand, in Figure 2, we have marked, with a symbol representing protected shields, the steps where security and privacy must be offered due to the data exchanged (considering the data classification presented above) in the steps or the operation processes performed on them. For example, the user authentication step into the EMR is a process that should be secured since an attacker could impersonate the patient to perform malicious activities.

Focusing on the LIS, *McCudden* et al. [25] conducted a complete review of the LIS with the different phases, elements, and critical factors that this component contains. Their work presents mainly two levels of security: access control and encryption, derived from GDPR and HIPAA directives, both explained in Section II-B. *McCudden* et al. [25] indicated that file and directory accesses are managed

TABLE 3. Classification of primary and secondary uses of health data.

***High** = High level of data criticality, **Very Sensitive** = Highest level of data criticality.*

Data use	**High**	**Very Sensitive**
Primary use	- No defined data	• Patient summaries • Electronic prescriptions • Electronic dispensations • Medical images and image reports • Laboratory results • Discharge reports
Secondary use	• Data impacting on health (social, environmental behavioural determinants) • Pathogen genomic data, impacting on human health • Identification data related to practitioners involved in the treatment of a patient • Feedback from data holders • Health-related administrative data (including claims and reimbursement data) • Population-wide health data registries (public health registries) • Questionnaires and surveys • Electronic Health Data (EHD) related to education, lifestyle, and wellness	• Electronic Health Records (EHR) • Person generated health data (medical devices, apps, etc.) • Human genetic, genomic, and proteomic data • EHD from medical registries for diseases • EHD from clinical trials • EHD from medical devices for medicinal products and devices • EHD from biobanks and databases

via access control lists. Regarding encryption, these authors provided two main mechanisms: file system-level encryption and full disk encryption. However, their work only presents general information related to security and privacy without commenting on any specific algorithm or mechanism in this environment. Therefore, there is a real need to contribute useful indications and statements to the clinical environment.

To cope with these needs, our paper aims to enrich the literature with the security and privacy mechanisms needed, considering the pathway model shown in this section.

IV. USE CASE THREAT MODEL

The use case defined in Section III might have different threats/attacks affecting its stakeholders. This enumeration of attacks is defined as a threat model for the clinical domain and is a novel contribution of this paper.

Bearing in mind the use case, the attackers could have different motivations: (i) monetary, the attackers use techniques to produce abnormal situations and ask for a ransom; (ii) extortion, the malicious actors gain access to sensitive data/operations and oblige professionals/patients to meet their conditions; and (iii) impersonation, the attackers can use identities stolen to buy, for instance, unauthorized drugs or medicines. These options motivate the attackers to compromise the use case through the threat model presented below.

Thanks to *López* et al.'s work [15], presented in Section II, a complete list of attacks affecting healthcare has been discovered. The contribution here is to identify the specific attacks focused on the clinical environment.

The threat model shown in Table 4 presents the list of attacks focused on the clinical environment defined. For each attack, the technical stakeholders affected (Instrument, Middleware, LIS, EMR, and Practitioner), the attack vector indicating if it needs physical access (PA) and user interaction (UI), and a brief description are indicated.

The first attack is *Malware*, a type of malicious software that aims to damage, disrupt, or gain unauthorized access to a computer system or network. All types of malware might affect the clinical environment, for instance, through a USB stick plugged into the final analyzer, spreading themselves into the laboratory (virus, worm, etc.), or legitimate software used on the laboratory computers (trojans).

The main malware type in the clinical use case is *Ransomware*. This type of malware encrypts critical patient data and demands a ransom for its release. Ransomware attacks on clinical environments can result in the loss or corruption of this information, leading to a significant disruption in healthcare operations and patient care. An example of its impact was the attack produced in the Clinic Hospital in Barcelona, which obliged to cancel 150 non-urgent operations and 3,000 appointments [47]. Moreover, this threat might disable the analyzers and produce concrete issues in the clinical sample life cycle pathway model.

Social engineering, *Phishing*, *Password intrusion*, *Impersonation*, *Unauthorized access*, and *Data breach* attacks are all interconnected and can lead to severe consequences in the clinical environment if not addressed promptly. One of the worst consequences is the unauthorized disclosure of sensitive patient information, as the data breach produced in the US by an unauthorized party that had access to certain system and removed copies of personal information [48], leading to severe violations of privacy and potential identity theft. *Social engineering* attacks are often used to gain unauthorized access to sensitive information or systems, mainly in the authentication-based stakeholders (Practitioner, EMR, LIS, and Middleware). Here, the *Password intrusion* attack might appear as another social engineering technique to force (brute force or through personal information obtained from the user) the user credentials. The EMR might be the main objective since it encompasses a great part of the sensitive patient data. *Phishing* attempts to mislead the practitioner, and it is the most prevalent cybersecurity threat in healthcare, as UpGuard company said in its annual report [49]. *Unauthorized access* attacks can occur when attackers exploit vulnerabilities in the technical stakeholders or use stolen login credentials to gain access to sensitive information. Finally, *Data breach* attacks are triggered when attackers successfully execute the Unauthorized access attack. The materialisation of this attack in the clinical use case can even damage the health of patients. Analyzing again the UpgGuard annual report, *Data breach* is located in the third position as one of the most

TABLE 4. Threat model for clinical sample life cycle pathway model (where PA = physical access and UI = user interaction).

Attack	Technical Stakeholder affected					Attack Vector		Description
	Instrument	Middleware	LIS	EMR	Practitioner	PA	UI	
Malware	✓	✓	✓	✓	–	✓/–	✓	Malicious software designed to compromise computer systems and networks.
Ransomware	✓	✓	✓	✓	–	✓/–	✓	Type of malware that encrypts data on a system and demands payment in exchange for the decryption key.
Social engineering	–	✓	✓	✓	✓	–	✓	Manipulate people into divulging sensitive information or taking actions that compromise security.
Phishing	–	✓	✓	✓	✓	–	✓	Technique used to trick people into giving up sensitive information such as login credentials or financial information.
Password intrusion	–	✓	✓	✓	✓	–	–	Gaining unauthorized access to a system by exploiting weak or compromised passwords.
Impersonation	✓	✓	✓	✓	✓	✓/–	✓/–	Used by attackers to pretend to be someone else, e.g., a healthcare professional, to gain access to sensitive information or systems.
Unauthorized access	✓	✓	✓	✓	✓	✓/–	–	Gaining access to a system or network without permission. It can be used to steal data or compromise security.
Data breach	–	✓	✓	✓	✓	✓/–	✓/–	A data breach is an incident in which sensitive information is exposed or stolen. It is a consequence of other attacks.
Firmware modification	✓	✓	✓	✓	–	✓	✓	It involves altering the firmware of a device to introduce malicious code or functionality.
Device cloning	✓	–	–	–	–	✓	–	Create an exact copy of a device, including data and software. It can be used to steal data or gain unauthorized access to systems.
Hardware trojan	✓	✓	✓	✓	–	✓	–	Malicious modification to a hardware device that can be used to steal data or compromise security.
SQL injection	–	✓	✓	✓	–	–	–	Exploit vulnerabilities in web applications and databases to steal data or compromise security.
Sniffing	–	✓	✓	✓	–	–	–	Intercepting network traffic to steal sensitive information or compromise security.
Tampering	✓	–	–	–	–	✓	✓	Act of modifying data or systems to steal information or compromise security.
Side channel	✓	–	–	–	–	✓/–	–	Exploit weaknesses in physical systems or devices to steal sensitive information.
Denial of Service	–	✓	✓	✓	✓	–	–	Overwhelming a system with traffic or requests to render it unusable.
Outdated OS	–	✓	✓	✓	–	✓/–	✓/–	Leave systems vulnerable to security threats and attacks due to lack of updates.

relevant attacks in healthcare, and subsequently in the clinical domain [49].

To continue, *Firmware modification* attack involves changing the software firmware of the device. The most potential stakeholder affected by this threat is the analyzer. However, the intruder should need physical access to this component. *Device cloning* attack entails creating a copy of a legitimate clinical device. The attacker here might leverage the cloned device to modify the analyzer operations or access sensitive data. Regarding *Hardware trojan* attack, an attacker could implant a hardware trojan in a medical device during the manufacturing process or through a supply chain attack, which involves introducing the trojan at some point in the supply chain. Traditionally, this attack can be focused on analyzers, but the rest of the technical stakeholders are also susceptible to suffering this kind of threat.

Focused on clinical databases, *SQL injection* targets databases by inserting malicious SQL statements into input fields, such as login forms, to gain unauthorized access to patient data or modify existing data in the database. The analyzer is excluded from this threat since it normally generates the record and sends it directly to the Middleware.

Sniffing attack involves eavesdropping data across a network. In this case, an attacker could intercept communications between all technical stakeholders. *Tampering* attack can occur when attackers modify medical records, clinical data, or device settings to cause harm to patients or disrupt clinical operations. Here, the main point to execute this attack is the analyzer since the whole clinical sample life cycle pathway model can suffer deviations with respect to the data obtained. Another attack focused on the analyzer is the *Side channel* attack. This threat uses the physical properties of a device, such as its electromagnetic emissions, to infer sensitive data.

To conclude, *Denial of Service (DoS)* and *Outdated OS* appear. On the one hand, *Denial of Service* consists of flooding a system with traffic or requests to overwhelm it, making it unable to function. This attack might cause worse effects depending on the visibility of the attacker in terms of the clinical landscape. In addition, the variation called *Distributed DoS* uses multiple computers synchronized to flood the technical stakeholder and cause an exponentially greater impact as the number of sources of the attack grows. This threat occupies the fourth position of the UpGuard annual report cited above [49]. On the other hand, the *Outdated OS* attack leverages the problem of clinical systems that are not updated or patched regularly, leaving them vulnerable to exploitation. This fact appears due to the proprietary software used by the technical stakeholders in many cases, some of which are unmaintained.

V. DEFINITION OF SECURITY AND PRIVACY REQUIREMENTS FOR CLINICAL SCENARIO

This section covers the needs identified in Section III-E, providing a comprehensive declaration of specific security and privacy requirements to satisfy the characteristics and procedures that appeared in the use case. Table 5 presents 22 requirements extracted from the definition of the clinical sample life cycle pathway model explained so far, as well as the threat model defined for it. The creation and validation of these requirements were based on the previous work, the EHDS, GDPR, and HIPAA regulations, as well as several on-site visits to a Spanish hospital where the functioning of these environments was verified and investigated.

In Table 5, the information provided for each requirement is: the requirement ID, marking some of them as optional; the description; the attacks covered, as identified in Table 4; the mapping of requirements with the steps shown in Figure 2; the technical security and privacy requirements obtained from *López* et al.'s work [15], presented in Section II-A, and also from the main regulations created by the US and EU; and finally, a novel definition of the protection mechanisms by the data uses levels (High and Very Sensitive) defined in Section III-D. This effort defines the minimum protection mechanisms to implement at each level.

The three first requirements in Table 5 are focused on authentication and access control to the clinical scenario. *R1* presents the need to authenticate internal and external users. *R2* and *R3* define that the use case must provide resource access, data, and services when the indicated users are needed, knowing the certain privileges/rights assigned. These requirements share CIA (Confidentiality, Integrity, Availability) and implement Authentication to verify users with valid credentials for *R1*; Resiliency, with the implementation of a security scheme to protect the assets even in the worst conditions for *R1*, *R2*, and *R3*; Authorization, to guarantee rights assigned to a user when is authenticated; and Identification, by assigning an identifier to users into the clinical environment for *R1* and *R2* as technical security requirements; in addition to EHDS, GDPR, and HIPAA compliance as privacy requirements.

R1, *R2*, and *R3* present similar protection mechanisms. On the one hand, all contain Blockchain-based mechanisms. Blockchain works with blocks, which store immutable and publicly available information inside this ledger. In general, many researchers have incorporated blockchain technology in clinical environments and healthcare [26], [51], [52], [53], [54], [55]. Highlighting the work performed in [54], they proposed the main advantages that this technology offers to healthcare data management systems, such as health data accuracy, health data interoperability, health data security, health data handling costs, global health data sharing, and improved healthcare data audit. Besides, different efforts have been performed to integrate blockchain with some of the protocols explained in Section III, such as HL7 FHIR, performed in [26]. In addition, some works address authentication and access control with blockchain, for instance, the work conducted in [56]. This work designed an architecture and an Advanced Signature-based Encryption algorithm to identify, secure, and authenticate healthcare IoT devices, using joint probability of IoT devices with random number generation. Regarding the type of blockchain to use, the work of *Mamun* [57] stated that a private blockchain, as opposed to a public blockchain, should be used in this environment since health information is critical and the performance of current public blockchains (Bitcoin, Ethereum, etc.) is limited.

On the other hand, the protection levels of *R1*, *R2*, and *R3* contain the levels proposed by the NIST in the NIST SP 800-63A and SP 800-63B, allocated into SP 800-63-3 "Digital Identity Guidelines" [58]. This document is selected due to the need to manage the patient's identity, and the NIST performs great work in such field. In this document, Identity Assurance Level (IAL) is defined as the identity proofing process; Authenticator Assurance Level (AAL) as the authentication process; and Federation Assurance Level (FAL) is referred to an assertion created to communicate the authentication and attribute information to a relying party (RP) [58]. IAL, AAL, and FAL implement three different categorizations regarding the protection needed.

Firstly, the NIST defines the IALs as follows:

- IAL1: there is no requirement to link the user to the person's identity in real life. The possible attributes used in the process are self-signed by the platform.
- IAL2: the user's identity must be remotely or physically identified. The attributes must be asserted by the Credential Service Provider (CSP) to the RP for pseudonymizing the identity.
- IAL3: the user's physical presence is necessary to demonstrate his/her identity. The CSP must assert the attributes to the RP for pseudonymizing the identity.

To continue, the NIST defines the AALs as follows:

- AAL1: the user is authenticated via single-factor or multi-factor authentication using available technologies, such as password-based credentials, facial recognition, or behavioural biometrics. The successful process must be demonstrated via a secure authentication protocol.
- AAL2: the authentication must be performed via two distinct authentication factors, requiring proof of possession, through secure authentication protocols. The successful process must be demonstrated via a secure authentication protocol.
- AAL3: the user is authenticated via a key through a cryptographic protocol. The authentication shall use a hardware-based authenticator and mechanisms to provide impersonation resistance.

Finally, the NIST defines the FALs as follows:

- FAL1: the RP receives a bearer assertion signed by the Identity Provider (IdP) using cryptography.
- FAL2: in addition to FAL1, the assertion must be encrypted. The RP is unique and can decrypt it.
- FAL3: the assertion has referenced a cryptographic key that must be presented for receiving the bearer assertion.

In this context, the three requirements *R1*, *R2*, and *R3* should implement AAL2 at the High level and AAL3 at the Very Sensitive level. For access control, if the federation is needed, FAL2 and FAL3 shall be implemented in *R2* and *R3* for High and Very Sensitive levels, respectively.

The following two requirements are *R4* and *R5*. *R4* can be traduced as the protection for "Data at Rest", and *R5*

TABLE 5. Definition of Security and Privacy requirements for clinical scenario.

Req. ID	Description	Attacks covered	Diagram step(s)	Technical Requirements		Protection Mechanisms	
				Security	Privacy	High	Very Sensitive
R1	The use case should authenticate either external (patients) or internal (practitioners, professionals, etc.) users in a secured and protected way.	Password intrusion, Phishing, Social engineering	1 and 2	CIA, Authentication, Resiliency, Identification	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based)	Blockchain-based, AAL3 (key-based)
R2	The use case must provide affordable resource access to certain users in function of the specific privileges/rights associated.	Unauthorized access, Data breach, Impersonation, DoS	3.1, 3.2, 3.3 and 17	CIA, Authorization, Resiliency, Identification	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2	Blockchain-based, AAL3 (key-based), FAL3
R3	The use case must provide personal EHR and related information when the indicated users as needed.	Unauthorized access, Data breach, Impersonation, DoS	3.3 and 16	CIA, Authorization, Resiliency	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2	Blockchain-based, AAL3 (key-based), FAL3
R4	The use case must protect and secure the data the different stakeholders share.	Sniffing, SQL injection, Tampering	3.3, 7, 9.2, 12, 13, 14.1, 14.2, 15.2 and 16	CIA, Resiliency	Anonymity, Unlinkability, Untraceability	RSA7680, ECDSA384, DH7680	RSA15360, ECDSA512, DH15360
R5	The use case must store the EHR and specific information securely and privately.	SQL injection, Malware, Ransomware	7, 14.1, 14.2 and 15.3	CIA, Robustness	EHDS, GDPR, HIPAA compliance	AES192, File system-level encryption	AES256, Full disk encryption
R6	The use case must collect and process the necessary data for patient billing.	SQL injection, Malware, Ransomware	14.4	CIA, Accountability, Resiliency	EHDS, GDPR, HIPAA compliance	Data protection (Cryptographic techniques)	Data protection (Cryptographic techniques)
R7	The use case must process and obtain the correct results from the patient sample collected.	Side channel, Firmware modification, Device cloning, Hardware trojan	12 and 13	CIA, Reliability, Resiliency, Fault tolerance, Robustness	EHDS, GDPR, HIPAA compliance	Anti-malware, IDS, Network isolation, Secure communications, Anomaly detection	Anti-malware, IDS, Network isolation, Secure communications, Anomaly detection
R8	The use case must register and track the test orders requested by the practitioners.	Sniffing, Tampering, Side channel	6, 8, 9.1 and 9.2	CIA, Non-repudiation, Accountability	Pseudonymity, Anonymity	Blockchain-based	Blockchain-based
R9	The use case must validate the result obtained from a sample by the analyzer.	Device cloning, Hardware trojan, Firmware modification	12, 13, 14.3 and 15.1	CIA, Robustness	Pseudonymity, Anonymity	Automatic verification (ML)	Semi-automatic verification (ML)
R10	The use case must protect the patient's personal and demographic information managed during all processes.	Sniffing, Tampering, Data breach	9.2	CIA, Resiliency	Pseudonymity, Anonymity	Data protection (Cryptographic techniques)	Data protection (Cryptographic techniques)
R11	The use case components must implement protection against the threat model defined.	ALL	All steps	CIA, Reliability, Resiliency, Fault tolerance, Robustness	EHDS, GDPR, HIPAA compliance	Anti-malware, Network isolation, Secure communications, IDS	Anti-malware, Network isolation, Secure communications, IDS
R12 (Opt.)	The EMR system should allow patients to authorize another person to access their EHRs.	Unauthorized access, Impersonation, Social engineering	3.1, 3.2, 3.3 and 17	CIA, Authorization, Accountability, Non-repudiation	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2	Blockchain-based, AAL3 (key-based), FAL3
R13 (Opt.)	The patient should request data rectification available into his/her EHR, as well as the right to be forgotten.	Unauthorized access, Impersonation, Social engineering	3.3 and 17	CIA, Authentication, Authorization	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2	Blockchain-based, AAL3 (key-based), FAL3
R14 (Opt.)	The patient may request the transmission of his/her EHR from the EMR system to another data recipient holder.	Unauthorized access, Impersonation, Sniffing, Tampering	17	CIA, Authentication, Authorization	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2, Secure communications	Blockchain-based, AAL3 (key-based), FAL3, Secure communications
R15 (Opt.)	The patient should restrict the access to healthcare professionals to his/her partial/all EHR information.	Unauthorized access, Impersonation, Social engineering	3.3	CIA, Identification, Authentication, Authorization	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2	Blockchain-based, AAL3 (key-based), FAL3
R16 (Opt.)	The patient may request information about the healthcare professionals that have access to his/her EHR.	Unauthorized access, Impersonation, Social engineering	3.3	CIA, Identification, Authentication, Authorization	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2	Blockchain-based, AAL3 (key-based), FAL3
R17 (Opt.)	The patient should be identified electronically using an electronic identification (From Regulation (EU) 910/2014 [50]).	Unauthorized access, Impersonation, Social engineering	1 and 16	CIA, Identification	EHDS, GDPR, HIPAA compliance	IAL2 (remote or physically presence)	IAL3 (physically presence)
R18	The use case must establish rules and mechanisms to comply with the data minimization principle (From Regulation (EU) 2016/679 [21]).	Data breach	9.2, 12 and 13	CIA	EHDS, GDPR, HIPAA compliance	Privacy-based mechanisms	Privacy-based mechanisms
R19	The EMR system must process health data for both primary and secondary use, as well as the transmission and management access to them	ALL	3.3, 7, 14.1, 14.2, 14.4 and 17	CIA, Authentication, Authorization	EHDS, GDPR, HIPAA compliance	Blockchain-based, Data protection (Cryptographic techniques)	Blockchain-based, Data protection (Cryptographic techniques)
R20	The EMR system must have a registry with the requests, accesses, and permissions granted to use patient EHR.	Unauthorized access, SQL injection, Password intrusion	3.3, 7, 14.1, 14.2 and 17	CIA, Accountability, Non-repudiation	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2	Blockchain-based, AAL3 (key-based), FAL3
R21	The EMR system must audit the controls, procedures, and user activities, and their use in the context of rights, standards, security, etc.	Outdated OS	1 and 17	CIA, Robustness	EHDS, GDPR, HIPAA compliance	Blockchain-based, AAL2 (two factor-based), FAL2	Blockchain-based, AAL3 (key-based), FAL3
R22	The LIS system must provide the health data anonymously. If not possible, the health data must be pseudonymized.	Data breach	9.2 and 13	CIA	EHDS, GDPR, HIPAA compliance	Privacy-based mechanisms	Privacy-based mechanisms

for "Data in Transit", the protection when the data are stored and when are transmitted. From *R5*, the Robustness security requirement is listed since the system must be implemented to cover possible abnormal situations. Besides, *R4* needs certain specific privacy requirements: Anonymity, by masquerading the information to hide user's identity; Unlinkability, to also hide the receiver of information; and Untraceability, to prevent the tracing of messages. All of them are linked with the process of transmitting data privately. Lastly, the protection levels are also particular for these two requirements and have been extracted from the US institutions since they explain in a more concrete format the algorithms to use in each case.

R4 is mainly protected by the digital signature algorithms to verify the authenticity of a document/file, the critical establishment of cryptographic keys for secure communication, and data in transit. In contrast, while R5 is protected with the algorithms of data at rest. The specific algorithms and their strength are established in the NIST SP 800-57 [59]. This document establishes as the two most substantial security values for Rivest-Shamir-Adleman (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA), Diffie Hellman (DH), and Advanced Encryption Standard (AES), the ones presented in the High and Very Sensitive columns of Table 5. RSA (Integer-factorization cryptography) and ECDSA (Elliptic-curve cryptography) are used for integrity protection and key establishment; DH (Finite-field cryptography) for key establishment; and AES for encrypting and decrypting data, mainly at rest.

The reason to apply the two most essential security values from SP 800-57 is that the US government establishes these two values for the data with Secret and Top Secret labels, the most restrictive information about its operations and processes as a country. On the other hand, R5 implements two types of encryption, file system-level encryption, and full disk encryption, to protect the High and Very Sensitive levels, respectively.

R6 references the billing process represented in Figure 2 with step 14.4 and requires the correct processing and transmission of metrics and parameters captured by the LIS to the EMR, such as procedure performed, result obtained, etc. Instead, *R7* is focused on the Middleware and Instrument part found in Figure 2 (steps 11 and 12), defending the correct procurement of results and protecting the machine in charge of analyzing the patient sample. As a new technical security requirement, *R6* demands Accountability, understood as the collection and maintenance of logs and processes performed, for example, with the samples from the patient to execute an accurate cost breakdown. On the other hand, *R7* needs Fault Tolerance as a security requirement not considered before. This requirement preserves the security of a system/environment even when a fault is produced. Here, the analyzer must be protected under any circumstance.

R6 and *R7* share the same privacy requirements as R1, R2, R3 and R5. To conclude these requirements, *R6* implements data protection mechanisms into the protection levels. Data protection can be traduced as the mechanisms showed in *R4* and *R5* (AES, RSA, etc.) to protect both communications and storage. In contrast, R7 implements different endpoint protection mechanisms, such as Intrusion Detection Systems (IDS), Anti-malware, Network isolation, Secure communications, and Anomaly detection. To classify these techniques, the FDA-2021-D-1158, created by the Food and Drug Administration (FDA) [60], has been analyzed in detail. This document presents different security control categories (event detection and logging, resiliency and recovery, etc.) and medical device recommendations. In this case, the High and Very Sensitive levels share the same mechanisms. The reason is that the Instrument (analyzer) and Middleware must be protected inherently for both protection levels. This requirement tries to resolve the problems in LIS1-A, LIS2-A2, and DICOM, implementing the protection mechanisms as an upper layer of such protocols.

R8 covers the need to register and track the test orders (CPOE) to know the steps, the people involved, and the processing performed on the sample. *R9* is focused on the step performed when the result is obtained and the validation to know if the result value is valid. The technical security requirements of *R8* and *R9* have been explained earlier. In this case, the privacy requirements include pseudonymity and anonymity to prevent the linkage of a patient with the test order or sample-derived results, but only when the results are uploaded to the EMR.

Regarding protection levels, R8 presents Blockchain as an alternative to satisfy this requirement. As commented above, Blockchain implements a ledger where the information is stored through immutable and public blocks. This characteristic allows the use case to track all tasks and processes performed with the sample. The work conducted in [61] presented the prominent use cases where Blockchain can be implemented in healthcare. They showed, for instance, the medical staff credential verification since each authentication procedure generates records stored in the Blockchain that can be examined. The work addressed in [61] also showed advantages like the transparency of Blockchain, security, etc., since all is recorded in the ledger. Finally, there are works combining SNOMED CT and Blockchain to better accurate medical decisions [62].

In the case of *R9*, it allocates automatic and semi-automatic verification as protection measures for High and Very Sensitive levels, respectively. Section III-C explained that the LIS validates the sample with different algorithms and rules installed. For the Very Sensitive level, a review by the authorized person may be necessary to control the correct validation and the non-exposure of personal data in the result obtained due to the criticality of this information.

Looking at Table 5, *R10* refers to the protection of personal and demographic (age, gender, religion, etc.) information managed in the use case. It needs CIA and Resiliency as technical security requirements and Pseudonymity and Anonymity as privacy ones. Regarding protection levels, this requirement R10 implements Data protection mechanisms, seeing the same ones presented in *R6*. *R10* is specially designed to cover the deficiencies found in the clinical protocols (LIS2-A2, HL7 v2, HL7 v3, etc.), which transmit demographic patient data without effective protection. On the other hand, *R11* lists the threat model created for this use case (Section IV), extracted from the work performed in [15]. In this case, R11 needs more security requirements and the abovementioned regulations as privacy requirements. For the protection levels, it implements the main protection mechanisms already presented in *R7*, which are IDS, Anti-malware, and Network isolation.

At this point, six requirements appear regarding user rights, from *R12* to *R17*. These rights have been extracted from EHDS regulation and are optional in their implementation, depending on the maturity of the solution to design. Firstly, *R12* presents the possibility of authorizing another person as the owner of information for accessing his/her EHRs; *R13* incorporates two rights listed in GDPR regulation, the data rectification and the right to be forgotten, understanding the former as the right to modify the personal data available in the EHR and the latter as the requesting of erasing patient data if the owner as needed; *R14* defends the right of the owner to transmit his/her personal information from one data holder to another; *R15* shows the possibility of restricting access to EHR to particular medical professionals if the data subject is requested; *R16* provides the ability to request information from professionals to access the patient's EHR. And finally, *R17* allows the use case to identify users with an electronic identification, listed in Regulation (EU) 910/2014 [50].

All the optional requirements appeared in Table 5, from *R12* to *R17*, practically share the same technical security and privacy requirements, taking into account Identification (uniquely identifying a person with a user) as a new requirement not considered above.

Regarding protection levels, the first five requirements demand to implement Blockchain for their protection, in addition to AAL2/AAL3 and FAL2/FAL3, the same mechanisms presented for *R2* and *R3*. Besides, there is a paradigm called Self-Sovereign Identity (SSI), which, together with Blockchain, can provide an effective implementation of these requirements. SSI allows patients full control over their personal data, eliminating the centralized third parties [63]. Implementing this paradigm would be an interesting future work to secure the clinical use case. To continue, *R17* implements the IALs categorizations explained above. In this case, *R17* develops IAL2 and IAL3, which require remote or physical identification and only physical identification to recognize the user, respectively.

To finish with the rights and GDPR principles, *R18* shows the data minimization principle to be included in this scenario. Firstly, GDPR defines data minimization as "the processing of personal data that is adequate, relevant and limited to what is necessary about the purposes for which they are processed" [64]. This requirement contains CIA and the privacy regulations for the security and privacy requirements. Concerning protection levels, privacy-based mechanisms are presented in both cases. These mechanisms cover pseudonymization, anonymization, generalization, suppression, and randomization techniques listed in the EHDS regulation. Besides, the work performed in [65] explored data minimization in healthcare in general and, therefore, in the clinical environment. *Mukta* et al. [65] presented different techniques to implement this principle: data masking (anonymize data); access delegation (data holder uses the data for only the purpose established); access control, selective disclosure (share only certain data); and consent management (data owner consent). Lastly, *Mukta* et al.'s [65] reviewed Blockchain as a technology to satisfy this principle in the medical domain.

Finally, four specific requirements (*R19*, *R20*, *R21*, and *R22*) appear for the EMR system of Section III-C. This system component manages and controls the EHR, the authentication, the medical procedures, etc., which must comply with the EHDS, GDPR, and HIPAA regulations from the implementation to the deployment into a clinical environment. *R19*, *R20*, *R21*, and *R22* require the correct processing or both primary and secondary use of clinical data, the registry of all operations and accesses performed with the patient EHR, the audit of controls, procedures, user activities and the compliance of user rights/standards/security, and the anonymization/pseudonymization of data allocated into the system. These requirements contain some of the technical security requirements already commented on above. Finally, the mechanisms presented in the protection levels are shared by the other requirements, such as Blockchain-based, data protection, AAL2/AAL3, FAL2/FAL3, and privacy-based protection mechanisms.

This contribution presents a baseline for protecting the use case operations/procedures and the identified clinical and health data uses. However, several mechanisms can have challenges in their adoption and implantation. For instance, Blockchain technology, which might increase operational costs in the short term, has a lack of legislative standards and issues in governance [66]. These challenges should be considered, but during this section, the benefits shown of using the enumerated technologies have the potential to improve the use case defined considerably, such as Data protection techniques, which can protect clinical data from data breaches. Regarding technologies selected, Blockchain appears as the most relevant technology, indicated in several requirements as a protection mechanism. This technology should be deeply addressed and studied in future work.

VI. CONCLUSION AND FUTURE WORK

The clinical environment presents quite challenges in security and privacy terms since it is one of the major sources of patient data for healthcare. In this work, the clinical sample life cycle pathway model has been created. As central contributions, a novel classification of clinical and healthcare data for their different uses has been created, dividing them into two sensitivity levels. In addition, the definition of security and privacy requirements for the use case have been established. In this context, different protection mechanisms have been assigned to the identified sensitivity levels after analyzing the official EU and US regulations.

As commented throughout the paper, the clinical environment suffers many cyber attacks. In the introduction, two sources were presented: insecure operations and security and privacy issues. Thanks to this article, many different deficiencies and points for improvement have been presented. Furthermore, this article has designed a list of security and privacy requirements to secure this environment effectively.

As future work, there are different lines to continue the research initiated in this article. Creating and standardizing new clinical protocols could directly impact the level of security and privacy in a clinical setting. Additionally, the definition of a practical testing environment could support all the knowledge concluded in our contributions. For that, searching for synthetic sources and open-source tools to represent EMR, LIS, etc. would help the implementation of the security and privacy requirements defined in this article.

Another line would be to study the secure technologies proposed, validating them into the testing environment previously deployed. For instance, Blockchain technology has been identified as one of the most promising ones. The idea would be to take advantage of the different benefits commented on above. In this context, a comprehensive study of the best blockchain solutions to include in the clinical use case would be needed, with their implementations, features, and requirements for an affordable deployment.

Finally, the evolution of the clinical use case presented here to a scalable and distributed environment could expand the set of requirements and technologies provided. Here, the SSI paradigm presented in Section V could enhance patient privacy, giving them control over their data and selecting who and when can access them.

REFERENCES

[1] S. Dash, S. K. Shakyawar, M. Sharma, and S. Kaushik, "Big data in healthcare: Management, analysis and future prospects," *J. Big Data*, vol. 6, no. 1, p. 54, Dec. 2019.

[2] The American Society for Clinical Laboratory Science. (2021). *Value of Medical Laboratory Science Personnel and Clinical Laboratory Services in Healthcare*. Accessed: Nov. 3, 2023. [Online]. Available: https://ascls.org/value-of-clinical-laboratory-services/

[3] McAfee. (2017). *Doctoring Data: Why Cybercriminals Have Their Eye on Healthcare*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.mcafee.com/blogs/privacy-identity-protection/healthcare-data-cybercrime/

[4] E. Kost. (2022). *13 Biggest Healthcare Data Breaches*. UpgGuard, Inc. Accessed: Nov. 3, 2023. [Online]. Available: https://www.upguard.com/blog/biggest-data-breaches-in-healthcare

[5] V. Hassija, V. Chamola, B. C. Bajpai, Naren, and S. Zeadally, "Security issues in implantable medical devices: Fact or fiction," *Sust. Cities Soc.*, vol. 66, Mar. 2021, Art. no. 102552.

[6] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "Digital healthcare–cyberattacks in Asian organizations: An analysis of vulnerabilities, risks, NIST perspectives, and recommendations," *IEEE Access*, vol. 10, pp. 12345–12364, 2022.

[7] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Trans. Comput. Healthcare*, vol. 2, no. 3, p. 27, 2021.

[8] D. F. Cowan, "Security and confidentiality on laboratory computer systems," in *Informatics for the Clinical Laboratory: A Practical Guide*. New York, NY, USA: Springer, 2005, pp. 59–86.

[9] S. Y. Ameen and I. M. Ahmed, "Design and implementation of e-laboratory for information security training," in *Proc. 4th Int. Conf. e-Learn. Best Practices Manage., Design Develop. e-Courses, Standards Excellence Creativity*, Cincinnati, OH, USA, May 2013, pp. 310–317.

[10] I. C. Cucoranu, A. V. Parwani, A. J. West, G. Romero-Lauro, K. Nauman, A. B. Carter, U. J. Balis, M. J. Tuthill, and L. Pantanowitz, "Privacy and security of patient data in the pathology laboratory," *J. Pathol. Informat.*, vol. 4, no. 1, p. 4, Jan. 2013.

[11] E. K. Leibach, "Autonomy and privacy in clinical laboratory science policy and practice," *Amer. Soc. Clin. Lab. Sci.*, vol. 27, no. 4, pp. 222–230, Oct. 2014.

[12] H. B. Rahmouni, I. Essefi, and M. F. Ladeb, "Enhanced privacy governance in health information systems throughbusiness process modelling and HL7," *Proc. Comput. Sci.*, vol. 164, pp. 706–713, Jan. 2019.

[13] I. Essefi, H. B. Rahmouni, and M. F. Ladeb, "Integrated privacy decision in BPMN clinical care pathways models using DMN," *Proc. Comput. Sci.*, vol. 196, pp. 509–516, Jan. 2022.

[14] H. Yang, J. Yuan, C. Li, G. Zhao, Z. Sun, Q. Yao, B. Bao, A. V. Vasilakos, and J. Zhang, "BrainIoT: Brain-like productive services provisioning with federated learning in industrial IoT," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 2014–2024, Feb. 2022.

[15] A. López Martínez, M. Gil Pérez, and A. Ruiz-Martínez, "A comprehensive review of the state-of-the-art on security and privacy issues in healthcare," *ACM Comput. Surv.*, vol. 55, no. 12, pp. 1–38, Dec. 2023.

[16] A. U. Patel, C. L. Williams, S. N. Hart, C. A. Garcia, T. J. S. Durant, T. C. Cornish, and D. S. McClintock, "Cybersecurity and information assurance for the clinical laboratory," *J. Appl. Lab. Med.*, vol. 8, no. 1, pp. 145–161, Jan. 2023.

[17] MITRE. (2023). *MITRE ATT&CK*. Accessed: Nov. 3, 2023. [Online]. Available: https://attack.mitre.org/

[18] U.S. Department of Health & Human Services. (1996). *Health Insurance Portability and Accountability Act*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.hhs.gov/hipaa/

[19] U.S. Food & Drug Administration. (2023). *FDA Cybersecurity*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

[20] National Institute of Standards and Technoloy (NIST). (2023). *Healthcare Standards & Testing*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.nist.gov/itl/products-and-services/healthcare-standards-testing

[21] European Parliament and of the Council. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Accessed: Nov. 3, 2023. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/2016-05-04

[22] European Parliament and of the Council. (2020). *Data Governance Act COM/2020/767*. Accessed: Nov. 3, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:767: FIN

[23] Directorate-General for Health and Food Safety. (May 2022). *Proposal for a Regulation on the European Health Data Space*. Accessed: Nov. 3, 2023. [Online]. Available: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

[24] R. Hussein, L. Scherdel, F. Nicolet, and F. Martin-Sanchez, "Towards the European health data space (EHDS) ecosystem: A survey research on future health data scenarios," *Int. J. Med. Informat.*, vol. 170, Feb. 2023, Art. no. 104949.

[25] C. R. McCudden, M. P. A. Henderson, and B. R. Jackson, *Contemporary Practice in Clinical Chemistry*, 4th ed. New York, NY, USA: Academic, 2020, ch. Laboratory Information Management, pp. 301–321.

[26] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Comput. Structural Biotechnol. J.*, vol. 16, pp. 267–278, Jan. 2018.

[27] Clinical and Laboratory Standards Institute. (2003). *LIS1-A1: Standard Specification for Low-Level Protocol to Transfer Messages Between Clinical Laboratory Instruments and Computer Systems*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.astm.org/e1381-02.html

[28] Clinical and Laboratory Standards Institute. (2004). *LIS2-A2: Specification for Transferring Information Between Clinical Laboratory Instruments and Information Systems*. Accessed: Nov. 3, 2023. [Online]. Available: https://clsi.org/standards/products/automation-and-informatics/documents/lis02/

[29] IVD Industry Connectivity Consortium. (2017). *Laboratory Connectivity Guide*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.cdc.gov/cliac/docs/addenda/cliac0418/15a_IIC_LA_an_LIV_Handout.pdf

[30] American Society for Testing and Materials. (2007). *Standard Practice for Content and Structure of the Electronic Health Record (EHR)*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.astm.org/e1384-07.html

[31] M. A. Hussain, S. G. Langer, and M. Kohli, "Learning HL7 FHIR using the HAPI FHIR server and its use in medical imaging with the SIIM dataset," *J. Digit. Imag.*, vol. 31, no. 3, pp. 334–340, Jun. 2018.

[32] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT communications: A survey," *Sensors*, vol. 20, no. 17, p. 4828, Aug. 2020.

[33] A. Celesti, M. Fazio, A. Romano, and M. Villari, "A hospital cloud-based archival information system for the efficient management of HL7 big data," in *Proc. 39th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2016, pp. 406–411.

[34] C.-M. Chituc, "An analysis of IoT interoperability standards in the healthcare sector," in *Proc. IECON 45th Annu. Conf. IEEE Ind. Electron. Soc.*, vol. 1, Oct. 2019, pp. 2910–2915.

[35] D. B. Ali, I. Ghorbel, N. Gharbi, K. B. Hmida, F. Gargouri, and L. Chaari, "Consolidated clinical document architecture: Analysis and evaluation to support the interoperability of Tunisian health systems," in *Digital Health Approach for Predictive, Preventive, Personalised and Participatory Medicine*. Cham, Switzerland: Springer, 2019, pp. 43–52.

[36] F. Pecoraro, D. Luzi, and F. L. Ricci, "The use of HL7 clinical document architecture schema to define a data warehouse dimensional model for secondary purposes," *Eur. J. Biomed. Informat.*, vol. 13, no. 1, pp. 85–95, 2017.

[37] R. Saripalle, C. Runyan, and M. Russell, "Using HL7 FHIR to achieve interoperability in patient health record," *J. Biomed. Informat.*, vol. 94, Jun. 2019, Art. no. 103188.

[38] N. F. Alves, L. Ferreira, N. Lopes, M. L. R. Varela, H. Castro, P. S. Ávila, H. A. Teixeira, G. D. Putnik, and M. M. Cruz-Cunha, "FHIRbox, a cloud integration system for clinical observations," *Proc. Comput. Sci.*, vol. 138, pp. 303–309, Jan. 2018.

[39] T. Benson and G. Grieve, "Security & integrity in FHIR," in *Principles of Health Interoperability*. Cham, Switzerland: Springer, 2021, pp. 193–210.

[40] T. Ecarot, B. Fraikin, F. Ouellet, L. Lavoie, M. McGilchrist, and J.-F. Ethier, "Sensitive data exchange protocol suite for healthcare," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–7.

[41] Open Medscience. (2022). *Digital Defenses in Radiology: Cyber Security in Medical Imaging Systems*. Accessed: Nov. 3, 2023. [Online]. Available: https://openmedscience.com/digital-defenses-in-radiology-cyber-security-in-medical-imaging-systems/

[42] Security A(r)twork. (2022). *Hacking DICOM: The Hospital Standard*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.securityartwork.es/2022/04/05/hacking-dicom-the-hospital-standard-2/

[43] Z. Wang, Q. Li, Q. Liu, B. Liu, J. Zhang, T. Yang, and Q. Liu, "DICOM-Fuzzer: Research on DICOM vulnerability mining based on fuzzing technology," in *Proc. Int. Conf. Commun. Netw.*, 2019, pp. 509–524.

[44] T. Benson and G. Grieve, "LOINC," in *Principles of Health Interoperability*. Cham, Switzerland: Springer, 2021, pp. 325–338.

[45] R. Khanna and T. Yen, "Computerized physician order entry: Promise, perils, and experience," *Neurohospitalist*, vol. 4, no. 1, pp. 26–33, Jan. 2014.

[46] C. Yan, Y. Zhang, J. Li, J. Gao, C. Cui, C. Zhang, G. Song, M. Yu, J. Mu, F. Chen, X. Han, and W. Cui, "Establishing and validating of an laboratory information system-based auto-verification system for biochemical test results in cancer patients," *J. Clin. Lab. Anal.*, vol. 33, no. 5, Jun. 2019, Art. no. e22877.

[47] B. Toulas. (2023). *Hospital Clínic de Barcelona Severely Impacted by Ransomware Attack*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/hospital-cl-nic-de-barcelona-severely-impacted-by-ransomware-attack/

[48] J. McKeon. (2023). *Biggest Healthcare Data Breaches Reported This Year, So Far*. Health IT Security. Accessed: Nov. 3, 2023. [Online]. Available: https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far

[49] E. Kost. (2023). *Biggest Cyber Threats in Healthcare*. UpgGuard, Inc. Accessed: Nov. 3, 2023. [Online]. Available: https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare

[50] European Parliament and of the Council. (2014). *Regulation (EU) 2014/910*. Accessed: Nov. 3, 2023. [Online]. Available: http://data.europa.eu/eli/reg/2014/910/oj

[51] Y. Luo, H. Jin, and P. Li, "A blockchain future for secure clinical data sharing: A position paper," in *Proc. ACM Int. Workshop Secur. Softw. Defined Netw. Netw. Function Virtualization*, Mar. 2019, pp. 23–27.

[52] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2169–2176, Aug. 2020.

[53] H. Mahmud and T. Rahman, "An application of blockchain to securely acquire, diagnose and share clinical data through smartphone," *Peer Peer Netw. Appl.*, vol. 14, no. 6, pp. 3758–3777, Nov. 2021.

[54] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, vol. 34, no. 14, pp. 11475–11490, Jul. 2022.

[55] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Comput. Netw.*, vol. 200, Dec. 2021, Art. no. 108500.

[56] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, "Identification and authentication in healthcare Internet-of-Things using integrated fog computing based blockchain model," *Internet Things*, vol. 15, Sep. 2021, Art. no. 100422.

[57] Q. Mamun, "Blockchain technology in the future of healthcare," *Smart Health*, vol. 23, Mar. 2022, Art. no. 100223.

[58] National Institute of Standards and Technology. (Feb. 2020). *NIST Special Publication 800-63-3 Digital Identity Guidelines*. Accessed: Nov. 3, 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/63/3/upd2/final

[59] National Institute of Standards and Technology. (May 2020). *NIST Special Publication 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 General*. Accessed: Nov. 3, 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

[60] Food and Drug Administration. (Apr. 2022). *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*. Accessed: Nov. 3, 2023. [Online]. Available: https://www.fda.gov/media/119933/download

[61] P. Tagde, S. Tagde, T. Bhattacharya, P. Tagde, H. Chopra, R. Akter, D. Kaushik, and M. Rahman, "Blockchain and artificial intelligence technology in e-health," *Environ. Sci. Pollut. Res.*, vol. 28, no. 38, pp. 52810–52831, Oct. 2021.

[62] A. K. Talukder, M. Chaitanya, D. Arnold, and K. Sakurai, "Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 257–262.

[63] R. Soltani, U. T. Nguyen, and A. An, "A survey of self-sovereign identity ecosystem," *J. Appl. Technol. Innov.*, vol. 2021, pp. 1–26, Jul. 2021.

[64] General Data Protection Regulation. (2022) *Art. 5 GDPR: Principles Relating to Processing of Personal Data*. Accessed: Nov. 3, 2023. [Online]. Available: https://gdpr-info.eu/art-5-gdpr/

[65] R. Mukta, H.-Y. Paik, Q. Lu, and S. S. Kanhere, "A survey of data minimisation techniques in blockchain-based healthcare," *Comput. Netw.*, vol. 205, Mar. 2022, Art. no. 108766.

[66] D. Singh, S. Monga, S. Tanwar, W.-C. Hong, R. Sharma, and Y.-L. He, "Adoption of blockchain technology in healthcare: Challenges, solutions, and comparisons," *Appl. Sci.*, vol. 13, no. 4, p. 2380, Feb. 2023.

ANTONIO LÓPEZ MARTÍNEZ is currently pursuing the Ph.D. degree in new technologies, specializing in cybersecurity, with the University of Murcia. He is working in virtualization technologies (docker and kubernetes) and the implantation of cybersecurity into the medical domain. His research interests include virtualization, privacy, security, and medical networks and domains.

MANUEL GIL PÉREZ received the M.Sc. and Ph.D. degrees (Hons.) in computer science from the University of Murcia, Murcia, Spain. He is currently an Associate Professor with the Department of Information and Communication Engineering, University of Murcia. His scientific activity is mainly devoted to cybersecurity, including intrusion detection systems, trust management, privacy-preserving data sharing, and security operations in highly dynamic scenarios.

ANTONIO RUIZ-MARTÍNEZ (Senior Member, IEEE) received the B.E., M.E., and Ph.D. degrees in computer sciences from the University of Murcia, Spain. He is currently an Associate Professor and an IT Coordinator with the Department of Information and Communications Engineering, University of Murcia. He is leading the Teaching Innovation Group, UMU, in the teaching of ICT and their fundamentals. His main research interests include electronic payment systems, security, privacy, and educational technology.