



# Are the Healthcare Institutions Ready to Comply with Data Traceability Required by GDPR? A Case Study in a Portuguese Healthcare Organization

Cátia Santos-Pereira<sup>1,2</sup><sup>a</sup>, Alexandre B. Augusto<sup>1</sup>, José Castanheira<sup>3</sup>, Tiago Morais<sup>3</sup>  
and Ricardo Correia<sup>1,4</sup><sup>b</sup>

<sup>1</sup>HealthySystems, Porto, Portugal

<sup>2</sup>Faculdade de Engenharia da Universidade do Porto, Porto, Portugal

<sup>3</sup>Unidade Local de Saúde de Matosinhos, Porto, Portugal

<sup>4</sup>CINTESIS – Centro de Investigação em Tecnologias e Serviços de Saúde, Porto, Portugal

**Keywords:** Audit-trail, Audit-log, GDPR, Security, Data Privacy, Traceability, Healthcare.

**Abstract:** GDPR introduces a new concept: "Data protection by design and per default" for new software development however legacy systems will also have to adapt in order to comply. This creates great pressure on health care institutions, namely hospitals, and software producers to provide data protections and traceability mechanisms for their current and legacy systems. The aim of this work is to understand the maturity level of a Portuguese Healthcare Organization in their audit records to comply with GDPR article 30 and 32 since healthcare organization operate in a daily-basis with personal data. This study was performed with the partnership of a public Portuguese healthcare organization and were organized into three main phases: (1) data collection of all information systems that operate with personal data; (2) interviews with IT professionals in order to retrieve the necessary knowledge for each information system and (3) analysis of the collected data and its conclusions. This study helped to identify a need inside this organization and to determine a follow-up plan to overpass this challenge. However it also identified some constrains like financial budget, legacy systems, small team of IT professionals in the organization and difficulties in establish communication with information system providers.


## 1 INTRODUCTION


In 2016, the European Commission proposed to replace the Directive (95/46/EC) (Européen et du Conseil, 1995) by the General Data Protection Regulation (GDPR) (Comission, 2016). The overall intention of this reform is to mitigate data access and security concerns giving citizens back control over their personal data, and to simplify the regulatory environment for business in the digital economy (Skendžić, 2018)

In order to ensure free secure flow of personal data, GDPR introduces a new concept: "Data protection by design and per default". This concept is applied to all products and services aimed or used in the European market must be designed with data protection in mind from the earliest stages of development (Colesky, 2016).

In particular the GDPR articles 30 and 32 focus in the importance of establish record of the activities and a process to operate over it in order to guarantee data security. Meanwhile the article 30 propose is to define the necessary information to establish a complete record for the activities, the article 32 target the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. The article 32 also states that organization shall define a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security (Comission, 2016), (Haug, 2018). This creates great pressure on healthcare institutions, namely hospitals, and software producers to provide auditable traceability mechanisms for their current and legacy systems (Gonçalves-Ferreira, 2018).

One way to apply traceability mechanisms is to implement audit log system. All actors such as information systems, processes, and services involved in

<sup>a</sup> <https://orcid.org/0000-0001-8425-6342>

<sup>b</sup> <https://orcid.org/0000-0002-3764-5158>

an auditable event should record an Audit Log. This will likely result in multiple Audit Log entries that show whether privacy and security safeguards, such as access control, are properly functioning across an enterprise's system-of-systems (Kong, 2012). Thus, it is typical to get an auditable event recorded by both the application in a workflow process and the servers that support them. For this reason, duplicate entries are expected, which is helpful because it may aid in the detection of. For example, fewer than expected actors being recorded in a multi-actor process or attributes related to those records being in conflict, which is an indication of a security problem (Margulies, 2015).

The content of an Audit Log is intended for use by security system administrators, security and privacy information managers, and records management personnel. This content is not intended to be accessible or used directly by other healthcare users, such as providers or patients, although reports generated from the raw data would be useful. An example is a patient-centric accounting of disclosures or an access report. Servers that provide support for Audit Log resources would not generally accept update or delete operations on the resources, as this would compromise the integrity of the audit record. Access to the Audit Log would typically be limited to security, privacy, or other system administration purposes (Jayabalan, 2017), (Kent and Souppaya, 2006).

Portugal has an extensive information infrastructure, which plays a central role in supporting healthcare provision, but not all data sources are effectively connected and some challenges in patient privacy and the legal basis for connecting patient data remain (Simões, 2017). Health Information Systems deployed in Hospitals or primary care units were mainly devoted to support local performed operational tasks and were implemented without an integrated perspective, leading with a great heterogeneity and data duplication (Pinto, 2016).

Ineffective data management, compliance issues, and cyber security risks are often linked with not having systematic approaches to investments in people, processes, and technology. Dated technology is everywhere and connected to everything— not just on desktop PCs. Many employees at hospitals, health plans, life sciences companies, and governments lack awareness of and training to manage financial, operational, compliance, and cybersecurity risks (Cooper, 2018).

These constitutes a major problem when health care institutions have to manage a vast amount of application, as observed in many public hospitals in Portugal.

Since the date of effect, GDPR takes at least ninety-one GDPR violations identified by data protection authorities around Europe, as published by CMS (CMS, 2019). Since not all fines are made public, this number cannot be complete. Inside healthcare sector at least two violations are reported, the fines and penalties are around 400.000 euros. The first identified GDPR violation in the healthcare sector happened in Portugal and was reported by the Portuguese Data Protection Authority. The investigation in *Centro Hospitalar Barreiro Montijo* revealed that the hospital's staff, psychologists, dietitians and other professionals had access to patient data through false profiles. Portuguese Data Protection Authority identified that the identity management system appeared deficient – since the hospital had 985 registered doctor profiles while only having 296 doctors. Moreover, doctors had unrestricted access to all patient files, regardless of the medical doctor's specialty. These issues events revealed violation of Article 5 (1) f) and Article 32 (CNPD, 2018) (Monteiro, 2019). The second case was reported by Dutch Supervisory Authority for Data Protection in Haga Hospital. It was detected a violation of Art. 32 GDPR (European Commission, 2016), because this Hospital does not implement a proper internal security of patient records in place. The investigation followed by Dutch Supervisory Authority for Data Protection concludes that dozens of hospital staff had unnecessarily checked the medical records of a well-known Dutch person (Peroonsgeevens, 2019).

The aim of this work is to understand the maturity level of a Portuguese Healthcare Organization in their audit records to comply with GDPR article 30 and 32 since healthcare organizations operate in a daily-basis with sensitive personal data. To achieve this goal it was selected a Portuguese Healthcare Organization and with the hospital Information Technology (IT) department collaboration it was compiled the characteristics of their information systems with a particularly focus in the audit-log records of the activities.

## 2 METHODS

In this section will be presented the methodology used to performed this study. In particular it will be presented the study design, the setting and participants.

### 2.1 Participants

This study was performed with the partnership of a public Portuguese healthcare organization (*Unidade Saúde Local*) constituted by a Hospital and 18 (eigh-

teen) primary care units. The Hospital has capacity for 342 beds. This organization provides healthcare services for more than 173.000 citizens. The main objectives of this organization are: (1) provide primary care and continuous health care to the county's population; differentiated healthcare to the population of the area of influence, and others that address it; (2) ensure public health activities and the means necessary for the exercise of competencies of the health authority in the county; (3) ensure the provision of primary, differentiated and continuous care, in and integrated way, embodying a *continuum* of patient-centered; and (4) promote the process of research and continuous education, pre and postgraduate, of sector, providing for the conclusion of agreements with the competent authorities.

### 2.2 Study Design and Setting

The study is organized into 3 (three) main phases, enumerated below:

1. Data collection of all information systems implemented that lead with personal data;
2. Interview with IT responsible with the objective of answer the following questions for each information system:
  - The information system has audit logs?
  - The audit logs are accessible by the organization?
  - The audit logs are structured?
  - Which are the content of the audit logs (e.g. applicational errors, access information)?
3. To analyse the collected information and systematize the results.

The interview was performed to the head of IT department and his team.

## 3 RESULTS

In this section it will be present the results of the study. First it will be presented the characterization of the Information systems implemented in the organization, then it was explored the audit logs available (structure and content), in the last sub-section it will be presented the audit logs access and use by the organization studied.

### 3.1 Information Systems Characterization

It were identified 64 (sixty-four) information systems in the organization that treat personal data (including both patients personal data and collaborators) from 23 (twenty-three) suppliers. The oldest information system was implemented in 1997 and since that year this organization started a dematerialization process until nowadays.

Fifty seven of all information systems are electronic medical information systems for the different departments systems (89%), five information systems with the purpose of employees management (8%) and only two information systems are for financial and logistic department (3%) as represented in Figure 1.

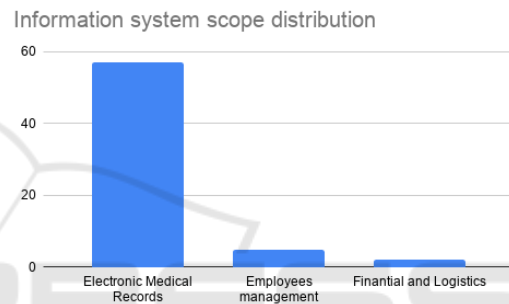


Figure 1: Information system scope distribution.

Regarding users, the majority of the users are medical doctors, administrative, nurses and diagnostic and therapeutic technicians. Others users were identified like IT and financial staff, nutritionist, pharmacists, social service, Insurer, library users, building security, formation, infrastructures, procurement, employee and also patients. This distribution is represented in Figure 2.

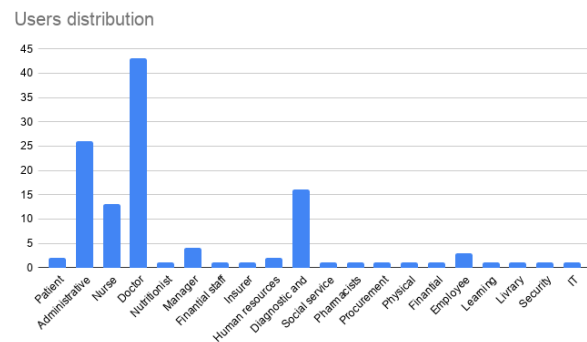


Figure 2: Users distribution.

In terms of data repository the majority of information systems are located inside the organization,

however thirty four percent of the information systems are located outside namely in ministry of health, North Regional Health Administration, an external organization and in the Portuguese Healthcare Regulation Authority as showed in Figure 3.

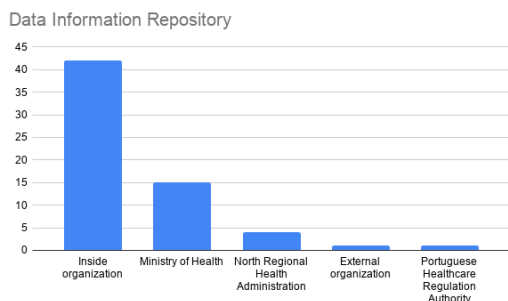


Figure 3: Data Information Repository.

### 3.2 Audit Logs

The results revealed that in the universe of sixty-four information systems, the organization only has access to audit logs from three information systems and from their interoperability platform that record logs from the communication between systems. The information system that provides audit logs are: (1) active directory; (2) Electronic Health Record, (3) Electronic medical system for women’s health care and a (4) interoperability platform.

One reason that explains this number is that thirty four percent of the sixty four information systems are located outside of the organization namely in the Portuguese ministry of health, North Regional Health Administration, an external organization and in the Portuguese Healthcare Regulation Authority.

In this subsection will be presented the three information system (active directory, electronic health record and electronic medical system for women’s health care) that contains audit logs and the interoperability platform which contain all events integrated between different information systems.

#### 3.2.1 Audit Logs Structure and Content

As mentioned before it will be present the audit logs structure and content for the three information systems and the interoperability platform.

- **Microsoft - Active Directory (AD)**

This system is a directory service developed by Microsoft, it authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

The organization studied implemented this technology to give support for the authentication and authorization of all collaborators in desktops inside the organization. AD allows to extract audit logs of the users activity, namely authentication and authorization in desktops but also in information systems that are integrated in AD.

This Microsoft tool allows to analyse and export the logs via Windows Event Viewer. The Figure 4 presents the audit record fields of authentication process and its descriptions.

Field	Description
account_name	User account that execute the action
computer_name	Computer name
account_domain	Account domain
category	Executed action category
description	Executed action description
detailed_authentication_information.key_length	Authentication key length
detailed_authentication_information.logon_process	Information of logon process
failure_code	Failure code
fingerprint	Unique identifier of event
host	Active directory hostname
level	Type of information
logon_type.logon_type	Number that represents how the user logon
network_information.client_address	Destination IP
network_information.client_port	Destination port
network_information.source_network_address	Source IP
network_information.source_port	Source port
network_information.workstation_name	Workstation name
new_logon.account_domain	Account domain - AD
new_logon.account_name	Account name (username)
new_logon.logon_guid	Unique code to correlate logon events on the computer
new_logon.logon_id	A semi-unique (unique between reboots) number that identifies the logon session just initiated
new_logon.security_id	Logon security unique ID
process_id	Unique ID of authentication attempt
process_information.process_name	Name of authentication attempt
service_id	Service unique ID
service_name	Service name
source_name	Source name
subject.account_domain	Account authenticated domain
subject.account_name	Account name authenticated
subject.logon_id	A semi-unique (unique between reboots) number that identifies the logon session just initiated
subject.security_id	Session unique ID

Figure 4: Audit log event - active directory.

- **Electronic Health Record - Sonho/Sclinico**

Sonho/Sclinico is the most used health information system used in this organization. This system gives support to outpatient, inpatient, operating room, ambulatory surgery, day hospital, primary care (outpatient) and primary care (emergency care) (Pavão, 2016).

The main end-users are medical doctors, nurses and nutritionist according to the different modules available.



The IT department of this organization, due to the relevance of this system, decides to start producing and collecting audit logs through database tables access.

The Figure 5 presents a sample of fields and it description of the EHR audit log available. In particular, It includes information about patient (patient record number), healthcare professional (identification, category, speciality, name, professional order number, internal number), characterization of access (IP, access type, timestamp) and characterization of actions (action code). This audit log is stored in a database table that was specially crafted by the Healthcare Organization in order to keep readable traceability records.

Field	Description
type	Information system identification
# cod categoria	Professional category code
# cod especialidade	Professional specialty code
data_log	Action timestamp
des categoria	Professional category description
des especialidade	Professional specialty description
des origem	Access type
endereco_ip	IP from source
fingerprint	Action code
# id_log	Professional action code
nome_prof	Username
# num_mec	Professional number
# num_ordem	Professional order number
# num_processo	Patient record code

Figure 5: Electronic Health Record log description.

• **Departmental Electronic Medical System: Women’s Health Care**

This Electronic Medical Record (EMR) has the specific goal of meet the need for an obstetric-specific record and is currently in use in the obstetrical/ gynaecological department. The main end-users are medical doctors and nurses.

The audit logs provided by this software vendor is under the GDPR requirements from article 30 by following the information requirement for a activity record.

The Figure 6 shows a sample of fields and it description that compose the audit log from this system. This audit log have more fields than the previous systems, beyond the identification of patient, healthcare professional and characterization of access, it also includes a more detailed information about what information was accessed and which actions were performed by the user. In order to access this audit log the organization needs to access the provider server and retrieve a JSON format file.

• **Interoperability Platform - HS.Helios**

The interoperability platform, HS.Helios, has the

Field	Description
type	Information system identification
acao.category	User Action Category
acao.details	Action details
acao.goal	Action objective
acao.id	Performed action
acao.justification	Action justification
acao.legal_basis	Legal basis of action
acao.timestamp	Action timestamp
dados.accessed_fields	Accessed data
dados.document_id	Document id accessed
dados.document_type	Document type
dados.source	Data source
proprietario.category	Data Owner Category
proprietario.id	Owner ID
proprietario.id_type	Owner ID type
receptor.category	Data receiver category
receptor.id	Data receiver ID
receptor.professional	Data receiver ID type
sistema_dados.department	Organization department identification
Sistema dados.ip	Data receiver IP
sistema_pedido.department	Organization department of owner
sistema_pedido.ip	Source IP
utilizador.category	User profile
utilizador.id	User ID
utilizador.id_type	Type of ID
utilizador.professional	Professional order number
utilizador.session_id	User session ID

Figure 6: Departmental Electronic medical system (women’s health care) log description.

ability to standardize and exchange health information like patient data from different informations systems. The most common format for data exchange in healthcare in Portugal is the Health Level 7 (HL7) version 2, also a newer version of HL7 known as Fast Healthcare Interoperability Resources (FHIR) starts gain some popularity. More than exchange health information, HS.Helios, also checks the integrity of exchanged messages and monitor the integrations in real time, allowing the extraction of performance metrics related to Health Information Systems integrations of distinct vendors. Furthermore it is also possible to create audit records of the exchanged messages. These audit records follows the Integrating the Healthcare Enterprise (IHE) Audit Trail and Node Authentication (ATNA) (IHE, 2019) format that complies with GDPR.

Figure 7 shows the systems that communicate through this interoperability platform, so it is possible to extract audit records of each integration (for example laboratory exams requisitions performed by EMR women’s health care information systems or laboratory exam requests and results that came from the emergency department). The platform also allow to consult these audit records

through a web platform allowing the institute to query over the audit records in a easy and simple way.

Bidirectional communications	
EMR women’s health care information system	Laboratory Information system
Email service	Interoperability Platform
Patient Care information system	Intensive care information system
Laboratory Information system	Emergency department information system
Electronic Health Record	Intensive care information system

Figure 7: HL7 communications recorded in audit logs.

Figure 8 presents the structure of audit-logs produced and available in interoperability platform. This records follows the structure audit event of the standard HL7 FHIR R4 (HL7.org, 2018) and is compliant with IHE-ATNA and GDPR establishing a strong format to produce well detailed activity record.

### 3.2.2 Audit Logs Access and Use by Organization

Concerning the access to audit records, the organization mentioned that they rarely access the logs or are asked to access it. It was also mentioned that very few professionals outside the IT department know that is even possible to collect this kind of data, and that if other professionals knew about that data maybe they would ask for it.

To access these audit logs the organization needs to access each systems individually as represented in Figure 9. The available of these audit logs is complicated (direct access to database tables or third party systems only used by IT department) and hard to understand for non-IT professionals, so the secondary use of data is conditioned.

## 4 DISCUSSION

After four years of preparation and debate in the European Union Parliament, the General Data Protection Regulation (GDPR) came into force in May 2018. Now, more than one year after the most important shift in data privacy regulation in 20 years approaches, widespread changes are already being felt in the healthcare industry, which is facing multiple challenges to protect sensitive data.

The overall results of this study reveals that the healthcare organizations are facing a complex chal-

Field	Description
Type	Event identifier
Sub-type	A more specific event identifier
Action	Action performance
Period	When the activity occurred
Recorded	Time when the event was recorded
Outcome	Event status
OutcomeDesc	Event status description
ProposeOfEvent	Event propose
Agent.Type	How the agent participated
Agent.Role	Agent role in the event
Agent.Who	Agent identifier
Agent.AltId	Agent alternative identifier
Agent.Name	Agent name
Agent.Requestor	A flag that indicates if the agent is the initiator
Agent.Location	Agent location
Agent.Policy	Policy that authorized the event
Agent.Media	Media type
Agent.Network.Address	Identifier for network access point of the user device
Agent.Network.Type	Type of network access point
Agent.PurposeOfUse	The reason given for the user
Source.Site	Logical source location
Source.Observer	Identity of source detecting the event
Source.Type	Source type where the event originated
Entity.What	Specific instance of resource
Entity.Type	Entity type
Entity.Role	What the role the entity played
Entity.Lifecycle	Life-cycle stage for the entity
Entity.SecurityLabel	Security labels on the entity
Entity.Name	Descriptor for the entity
Entity.Description	Descriptive text about the entity
Entity.Query	Query parameters
Entity.Detail.*	Additional information about the entity

Figure 8: Audit log event - interoperability platform.

lenge. This healthcare organization as many others even in different sectors in Portugal have a huge number of legacy information systems to manage. Some of information system providers already bankrupt and it is not possible to update the service. These difficulties allied to financial budget constraints constitutes a hard work to complete. During the study the organization became more aware of their difficulties, mainly in the complexity in access the audit logs since many of systems did not have audit logs available and even two of three systems (Sonho/Sclinico EHR, Electronic medical system for women’s health care, MS Active Director) that have audit logs were not fully compliant with article 20 of GDPR in their installed versions.

In an universe of sixty four information systems, at the moment of the study they only could access three of the information systems and their interoperability platform. As mentioned before twenty two of

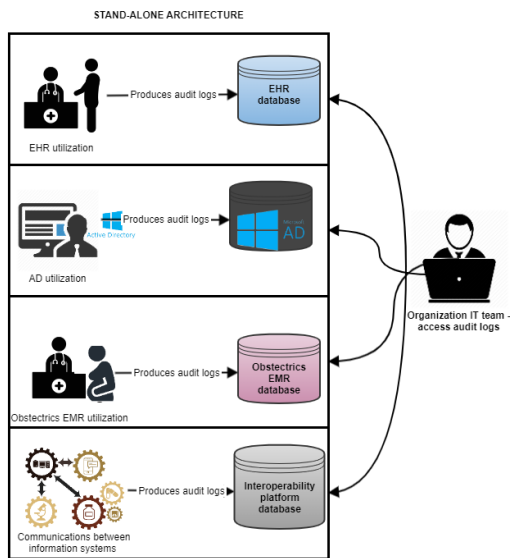


Figure 9: Stand-alone architecture of audit logs recorded.

the sixty four information systems are located outside of the organization with the responsibility of governmental unities or even external institutions, so for this systems the challenge is even worse.

Following these results, the organization IT responsible started communications with all information systems providers and the governmental unities requiring for access the audit logs. In order to facilitate the communication this organization used as gold standard for audit log structure and content, the Portuguese Resolution of the Council of Ministers n.º 41/2018 - RCM (Presidencia do Conselho de Ministros, 2018) which was designed following GDPR security requirements.

The Portuguese Government considered it is essential to define technical guidelines for the Public Administration, recommending them to the business sector, in the area of security architecture for information and procedures to be adopted to comply with GDPR standards. A part of this document is dedicated to traceability and audit logs.

The organization in study uses this information to require to providers to facilitate the audit logs with at least the following fields: (1) who access information, (2) from where were accessed (IP and Port), (3) when accessed, (4) which data were accessed and (5) which action were performed (create, read, update and delete). Until the moment of this work was submitted the organization does not had any answer among providers.

Another important aspect analysed in this study was the difficult that the organization had to analyse the available audit logs since they stay in a stand alone

architecture with different ways to access the records (tables in databases, third party applications, files and web platform). As a consequence the organization does not have the means to access the information in a friendly end-user interface.

The organization also identified that would be interesting cross information from the Active Directory (authentication) and the information systems, for example to create the patient journey or to calculate the length of sessions and activity in health information systems. This kind of indicators could help the organization to identify suspicious cases of usage (like credentials sharing) and effectively act for the creation of better security policies. To achieve this goal the organization will need to implement an audit trail solution that aggregate the audit logs from every information systems that leads with personal data and then work in indicators specification in order to have a daily basis traceability of events and alarmistic associated with suspicious cases. By archiving this goal the organization will comply with the article 32.

In sum, this study helped to identify a need inside this organization and to determine a follow-up plan to overpass this challenge. However it also identified some constrains like financial budget, legacy systems, small number of IT professionals in the organization and difficulties in establish communication with system providers.

## 5 CONCLUSION

This study constitutes a small part of the necessary audit work inside the organization. The results showed how difficult is for a public healthcare organization to carrying out and implement GDPR requirements. For one hand they have severe financial constrains and small team of IT professionals that difficult all the work and in the other hand due the non-structured dematerialization they have to lead with legacy information systems, that do not follow the standards and implement a vast amount of old technologies creating a difficult barrier to overcome. Despite all the effort observed from the IT professionals of the organization there is still a long and complicated path ahead in order to be complied with GDPR. It is also important remember that the articles 30 and 32 are only a fraction of GDPR. Healthcare organizations should be readying themselves to ensure their compliance with the new requirements of the GDPR by taking steps to understand their existing position.

Identifying a security committee and start carry out a readiness audit in the organization is a important step to take in order to provide an overview of compli-

ance gaps, and then risk rating those gaps against the likelihood of becoming a GDPR breach. This should be seen as the start point to define a list of recommendations in order to mitigate the risks of GDPR non-compliance. This study also identified the heterogeneity of the audit logs as a constraint since every information system analysed has a different method to access their audit logs and even a different format. In order to access these audit logs it was necessary to interview different IT professionals (a Database Administrator to access the database, System Administrator to retrieve the file and the AD event viewer and the integration specialist to access the integration platform). This complexity in accessing the audit logs showed the importance of having an audit trail platform to aggregate these audit logs in a common format in order to access it.

The future work includes a comparison between audit logs available and the GDPR and Portuguese Resolution of the Council of Ministers n.º 41/2018 requirements. After this work it will be needed to define a common format to homogenize and convert the audit logs to a single format in order to facilitate work with the audit logs in the organization.

## ACKNOWLEDGEMENTS

This article is a result of the project Demonstrator HS.REGISTER (NORTE-01-0247-FEDER-033756), supported by Competitiveness and Internationalization Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF). It was also supported by FCT (Fundação de Ciência e Tecnologia) through the doctoral fellowship [SFRH/BDE/105533/2014].

## REFERENCES

- CMS (2019). GDPR Enforcement Tracker.
- CNPD (2018). Deliberação N.º 984/2018.
- Colesky, M. (2016). Privacy shielding by design — a strategies case for near-compliance. In *2016 IEEE 24th International Requirements Engineering Conference Workshops*, pages 271–275.
- Commission, E. (2016). General Data Protection Regulation. *European Commission*.
- Cooper, T. (2018). 2018 Global health care outlook: The evolution of smart health care. *Deloitte*, pages 1–31.
- European Commission; (2016). Art. 32 GDPR Security of processing.
- Européen et du Conseil, P. (1995). Directive 95/46/CE.
- Gonçalves-Ferreira, D. e. a. (2018). Hs. register-an audit-trail tool to respond to the general data protection regulation (gdpr). *Studies in health technology and informatics*, 247:81–85.
- Haug, C. J. (2018). Turning the Tables — The New European General Data Protection Regulation. *New England Journal of Medicine*, 379(3):207–209.
- HL7.org (2018). Audit Event - HL7 FHIR.
- IHE (2019). IHE IT Infrastructure Technical Framework Volume 2a Transactions Part A –. *IHE International, Inc*, 2.
- Jayabalan, M. (2017). A design of patients data transparency in electronic health records. In *2017 IEEE ISCE*, pages 9–10.
- Kent, K. and Souppaya, M. (2006). Guide to Computer Security Log Management. *Nist Special Publication*.
- Kong, W. (2012). Process improvement for traceability: A study of human fallibility. In *2012 20th IEEE International Requirements Engineering Conference (RE)*, pages 31–40.
- Margulies, J. (2015). A developer's guide to audit logging. *IEEE Security Privacy*, 13(3):84–86.
- Monteiro, A. M. (2019). First GDPR fine in Portugal issued against hospital for three violations.
- Pavão, J. (2016). Usability study of clinico. In *2016 11th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6.
- Persoonsgegevens, A. (2019). Haga beboet voor onvoldoende interne beveiliging patiëntendossiers.
- Pinto, E. (2016). Identification and Characterization of Inter-Organizational Information Flows in the Portuguese National Health Service. *Applied clinical informatics*, 7(4):1202–1220.
- Presidência do Conselho de Ministros, P. (2018). Resolução do conselho de ministros n.º 41/2018.
- Simões, J. e. a. (2017). Health System in review -HiT- Portugal. Technical Report 2, European Observatory on health Systems and Policies.
- Skendžić, A. (2018). General data protection regulation — protection of personal data in an organisation. In *2018 41st MIPRO*, pages 1370–1375.