Journal of Universal Computer Science, vol. 27, no. 7 (2021), 650-666
submitted: 18/5/2020, accepted: 26/5/2021, appeared: 28/7/2021

Enhancing GDPR compliance through data sensitivity and data hiding tools

Xabier Larrucea
(TECNALIA, Basque Research and Technology Alliance (BRTA), Bizkaia, Spain
https://orcid.org/ 0000-0002-6402-922X, xabier.larrucea@tecnalia.com)

Micha Moffie
(IBM Haifa, Israel
moffie@il.ibm.com)

Dan Mor
(IBM Haifa, Israel
danm@il.ibm.com)

Abstract: Since the emergence of GDPR, several industries and sectors are setting informatics solutions for fulfilling these rules. The Health sector is considered a critical sector within the Industry 4.0 because it manages sensitive data, and National Health Services are responsible for managing patients' data. European NHS are converging to a connected system allowing the exchange of sensitive information cross different countries. This paper defines and implements a set of tools for extending the reference architectural model industry 4.0 for the healthcare sector, which are used for enhancing GDPR compliance. These tools are dealing with data sensitivity and data hiding tools A case study illustrates the use of these tools and how they are integrated with the reference architectural model.

Keywords: Health information management, industrial communication, data security, privacy, data processing
Categories: D.2.2, H.3.5, H.4.2
DOI: 10.3897/jucs.70369

1 Introduction

The healthcare sector is highly influenced by the General Data Protection Regulation (GDPR) [The European Parliament And Of The Council, 2016]. This is basically and partially due to the fact that healthcare management systems are being supported by computers where medical records and personal data are being processed. Systems must guarantee some degree of protection to stakeholders and some technologies are being used in this sense. Healthcare is being considered as a relevant topic within the Industry 4.0 [Celesti et al., 2019], which was defined back in 2011 [Pfeiffer, 2017], and it has been related to manufacturing or production processes. However, the medical field [Javaid and Haleem, 2019] is being considered as a part of Industry 4.0 [Badri et al., 2018]. In fact, Industry 4.0 and healthcare services [Alloghani et al., 2018] are complementary approaches and their integration and interoperability are becoming a need.

According to [Pang et al., 2018], *Industry 4.0 is spilling out from manufacturing to healthcare,* and the increase of digitally networked and data-intensive are pushing forward the smarter production concept and, thus, the industry 4.0 concept.

Since the emergence of the GDPR, the use of new technologies such as Internet of Things (IoT), cloud/fog/edge computing, big data analytics, artificial intelligence, and robotics in the medical sector is not banal nor straightforward.

This industry is moving to an integrated set of digitalized healthcare products and digitalized healthcare services. The integration of different technologies with healthcare systems is representing a major challenge especially when dealing with patients health records [Elhoseny et al., 2018], and its alignment to GDPR rules.

European citizens are entitled to move freely to different European countries, and each country has its own particularities concerning medical treatments and medical data management rights [Wismar et al., 2011]. Medical Data management including transfers of personal data to third countries or international organizations are major subjects within this European law, and mechanisms must be set up for assuring security and privacy, especially when managing patient's health records [The European Parliament And The Council Of The European Union, 2011].

However, the European Commission is promoting a set of services for connecting NHS from different countries in order to allow access and exchange European patients' medical records [Hathaliya et al., 2019] abroad. One of these services is the OpenNCP [European Commission, n.d.-b] which is a platform connecting National Health Services (NHS) cross European countries. Each country is connected throughout a set of services to the rest of national contact points in order to create a network for sharing patient's health records. Each NHS has a complex architecture and may be connected to Industry 4.0 technologies and/or IoT based architectures.

The connection of different NHS across Europe is a complex scenario requiring a defined and validated framework. Several research works have been done in this sense [Staffa et al., 2018], [Health information Institute, 2010], or they are ongoing [EHDEN consortium, 2020] in order to solve or to reduce the challenges for the healthcare sector [Lezzi et al., 2018]. Taking into account this scenario and our recent published works in this sense [Larrucea et al., 2020] and [Assaf et al., 2019]. We have introduced the use of policies, a consent management tool, a data hiding tool and a data sensitivity tool. Therefore, this paper contributes to this scenario with the following:

- Policy definition and use of a consent management tool
- Data Sensitivity tool integration within the healthcare industry 4.0 architectural model
- Data hiding tool integration within the healthcare industry 4.0 architectural model
- A case study illustrates the use of the architecture and the use of its related tools.

This paper is structured as follows. First, a background overview on healthcare, OpenNCP and GDPR, is provided. Second, the integration of data hiding and data sensitive analysis tools within the healthcare industry 4.0 architecture is proposed. Next, we define the case study to illustrate the approach. In section Five, we draw conclusions and outline future steps.

2 Background

2.1 Security and interoperability in Healthcare information systems

National healthcare systems are keystones for any country, but its security must be enhanced from a security perspective. Nowadays citizens are moving around the world travelling from one country into another, and there is an increasing need to provide them better support when they are travelling abroad. Therefore, interoperability is a challenge in healthcare systems. From a technical point of view, medical doctors must have access to patients' data by using the National Health Service (NHS) in order to figure out the patient's condition for improving diagnosis and treatments. In addition, this data must be available but there are several technical barriers such as the interoperability of patients' health records. As stated by [Wismar et al., 2011], NHSs are differently managed and implemented within the European Union. Therefore, if we want to allow the exchange of health records between countries, we need to provide the means for enabling their interoperability. Due to the complex set of systems involved within a NHS, we identified a healthcare industry 4.0 architecture [Larrucea et al., 2020] allowing us to define and use different tools for different purposes, as it was defined by the industry 4.0 environment [Schweichhart, 2016]. It's a relevant layer within the reference architectural framework [Schweichhart, 2016].

From a non-technical point of view, security awareness and training are some of the topics to be addressed in healthcare systems because this kind of systems are integrating a wide diverse set of technologies such as IoT systems [Pace et al., 2019].

As stated previously, there is a large number of initiatives dealing with this topic. However, our approach is to build upon the OpenNCP platform [European Commission, n.d.-b] a set of tools for enhancing security at data level where patient's health records are exchanged across European countries. This OpenNCP platform is supported by the eHealth Digital Service Infrastructure (DSI) Operations [European Commission, n.d.-a] directly managed by the European Commission. The purpose of the OpenNCP is to provide a common network and an infrastructure to connect different national healthcare systems. This initiative was launched by the epSOS project ['Smart Open Services for European Patients', 2018]. The eHealth DSI (eHDSI) is the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility (CEF). Each National Contact Points (NCP) for eHealth (NCPeH) is deployed in a VM which connects the others VM. In its turn, each member state has a complex and different infrastructure connecting the OpenNCP [Larrucea et al., 2019].

2.2 GDPR, eHealth records and consent

The General Data Protection Regulation (GDPR) [The European Parliament And Of The Council, 2016] is a European directive (law) where security aspects related to personal data must be enhanced. This is especially relevant in health-based systems because they are using personal data. When a European citizen travels abroad, and he is moving across European countries, they keep the same rights as in those from their origin countries. The management of personal data is considered as one of the main

challenges or topics to be addressed. In this context, the consent given by a citizen/patient is stressed by the GDPR where a controller must demonstrate that a patient gave its consent [The European Parliament And Of The Council, 2016]. This consent must be also exchanged among different member states when a patient is being assisted by a doctor in other country. The GDPR requires the management of this consent and privacy rules [Rios et al., 2019]. As health records are sensitive information, governments and agencies must establish the appropriate mechanisms as requested by the law. In this context, as patient's health records [The European Parliament And The Council Of The European Union, 2011] are exchanged, they should be connected to medical devices, hospitals records, and so on. Medical doctors require as much information as possible, and patients' information must be available.

GDPR and patients' health records related directive stress the consent management concept which is usually captured and evidenced by a piece of paper. Sometimes there is no evidence of the explicit consent, but healthcare systems require to capture the informed consent from patients in an explicit way. Consent management systems must define a specific consent architecture [Heinze et al., 2011].

It is worth to mention the need for connecting the GDPR and the possibilities of technological tools in support of legal compliance. This step represents a step forward on considering the legislative obligations. There are several research works such as [Pocs, 2012] where a legal scholar is dealing with this issue. Another example is [Conley and Pocs, 2018] where authors are analyzing the GDPR compliance challenges within interoperable health information exchanges.

3 Healthcare industry 4.0

3.1 Introduction to Healthcare industry 4.0 Architecture

As stated previously our work is based on the use of a healthcare industry 4.0 reference architecture [Larrucea et al., 2020]. Basically, this architecture defines the following layered stack (Figure 1):

- Business Processes: this layer involves the interaction among the different stakeholders to provide an added value to the healthcare industry 4.0 stakeholders. This layer considers the consent management process to illustrate how it works since consent has a relevant role within the current regulations such as the GDPR.
- Functions: to implement consent management functionalities, we need to develop and set up processes to (1) identify the sensitive data elements and (2) enforce the consent decision – in addition to the consent management tool *per se*. In particular, Healthcare systems must adhere to regulation. During interaction between different healthcare systems as well as the explicit consent stated by patients.
- Data: this layer deals with the format of the data exchanged and managed., This layer is related to the data required by the OpenNCP architecture. This architecture uses HL7 as the standard format. This layer deals with the format of the data, and the identification of the data.

- Communication: we are using the OpenNCP as a communication channel for sharing patients' information such as eHealth records. We extend the OpenNCP to include all different healthcare systems.
- Digitalization: health records are represented using HL7 and following the International Patient Summary guidelines. Scans and other medical results such as blood analysis are digitalized.
- Physical Things: Mobile devices can access health records by using encrypted channels. This aspect is not addressed in this paper due to space limitations.

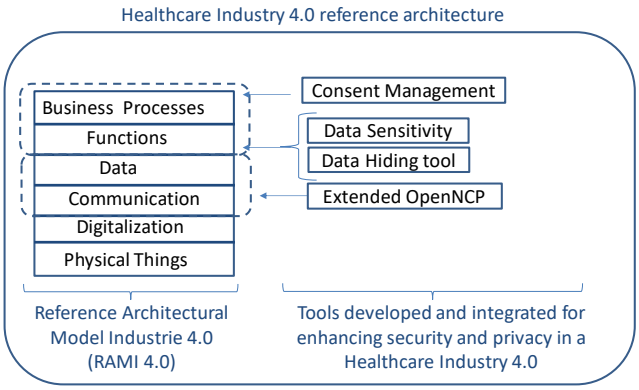

Figure 1: Reference Architectural Model Industry 4.0 adopted for the healthcare industry 4.0 [Larrucea et al., 2020]

3.2 Consent Management tool

Our approach is to use the consent management tool provided by Symphonic ['Symphonic', 2020], and to create a policy based on this tool. The following Figure 2 summarizes the main components of the consent management tool.

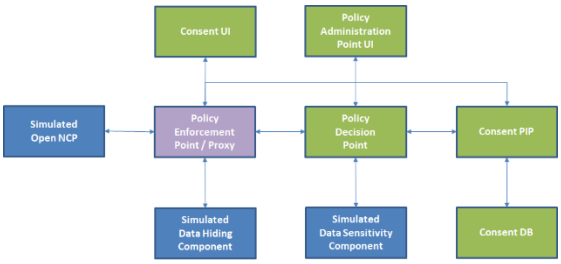

Figure 2: Consent Management tool

This tool has a Policy Manager containing a set of tools for implementing fine-grained and dynamic access control policies. This aspect allows us to govern how the resources such as medical records may be used. This manager is an ABAC (attribute based access

control) system, and it tries to answer the question: "*given the facts I know about the user, the resource being accessed, what the user wants to do with the resource, how sure I am the user is who she says she is, and any other pertinent facts about the world at this point in time, should the user's access request be permitted, and is there anything else that must be done in addition to permitting or denying access?*".

The following Figure 3 represents an overview of the tool where policies are defined and stored.

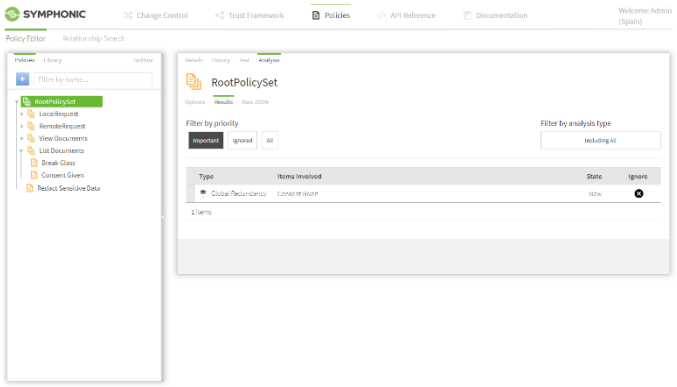

Figure 3: Consent management tool - policies

This tool is the upper layer of the healthcare industry 4.0 architecture [Larrucea et al., 2020], and it refers to the consent management which is one of the major issues [Asghar et al., 2017] in healthcare systems. Sometimes, remote consent is required when patients are travelling, and they are not physically present for giving consent. Consents requires the access to patient data [David et al., 2014], and physicians must deal with ethics and regulatory aspects such as GDPR. In fact, data processing of health information among different actors (e.g. peer to peer) [Weber-Jahnke and Obry, 2012] is the other major issue [Asghar et al., 2017], and this is especially relevant in emergency contexts [Shapiro et al., 2016] or even in the IoT (Internet of Things). Consent and policies [Karat et al., 2009] depend on the context [Russello et al., 2008]. In this sense, our approach based on [Buchanan et al., 2013] is to provide an integrated set of tools that supports and enables the creation of a formal structure for abstraction, governance and implementation of trust relationships and security policies.

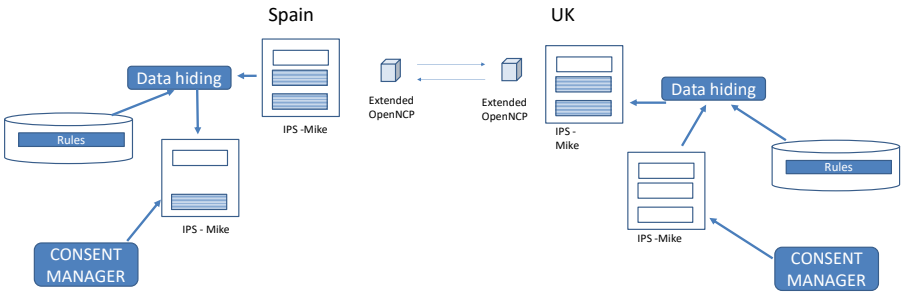

Figure 4: Business process flow and the interaction among data hiding tools and consent management

Figure 4 summarizes the workflow over two countries, and how the consent and the data hiding tool are used. Consent manager reads the patient's health records, and it stores the consent for each patient. Each consent is translated, and it is read by the data hiding tool. Then this tool masks the data fields based on the information stored within each consent. Afterwards the information is sent to the requested country by using the extended OpenNCP functionalitiy. Further explanation about this tool can be obtained here [SHiELD project, 2017].

3.3 Data hiding and data sensitivity tools

How does the Data hiding tool work?

The data hiding tool aims at addressing privacy rules related to sharing and storing of personal sensitive information – while providing a solution for real-world applications and data flows. The tool supports a wide range of data flows shown in the next figure. These flows (Figure 5) include: (1) Static data masking in DBs, (2) DB Response masking (3) Application layer masking (via proxy) where the traffic is monitored (via a proxy) and masked, (4) Log file masking and (5) Data export (e.g. to the cloud) and masked.

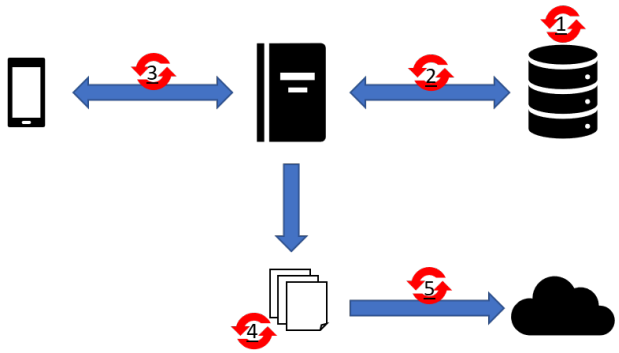

Figure 5: Common data flows – architectural view

While the use cases span a wide array of architectural and data flow arrangements the data hiding tool is designed to address the following common requirements:

1. Support a wide array of mechanisms to identify and select (sensitive) data elements within structured documents (e.g. xml, json, csv, xslx), unstructured documents (e.g. text, pdf, docx) as well as composite documents (e.g. HTML embedded within XML).
2. Provide a wide array of masking/unmasking operations including redaction, tokenization, encrypt, format preserving tokenization and format preserving encryption.to address different needs such as referential integrity and/or reversibility.
3. Support the modification (rewriting) of the payload itself while keeping its structure.
4. Provide the user with fine grained control over the tool behavior, e.g. using a policy.
5. Support for conditional and predicated processing.

To support these requirements the hiding tool (internally) constructs – based on the policy - masking/unmasking 'engines'. These engines handle (composite) payloads by processing the payloads in discrete steps. Essentially creating a flow of data where each step handles one aspect of the payload and postpones the rest of the processing for the next steps. In the design, we implement the data flow as a directed acyclic graph. The graph nodes are responsible for processing a specific type of payload. For example, a processor can be responsible to parse a JSON payload or encrypt text. The graph edges are responsible for (1) identifying the next processor in the data flow, (2) selecting a data element such as a Json element or a CSV Cell, and (3) providing the user with the ability to specify whether processing should be performed on the selected value (using predicates and conditions) based on additional input and/or the selected value itself.

To explain the tools, we present an example where the user would like to mask the name in the payload depicted in Figure 6. The steps to be taken are the following:

1. Parse XML, select XPath (e.g. "/partial-response/changes/update")
2. Parse Html, select CSS (e.g. "table > tbody > tr > td:nth-child(2)")
3. Mask content
4. Rebuild HTML with updated text
5. Rebuilt XML with updated element

```
<?xml version="1.0" encoding="utf-8"?>
<partial-response>
... <update ...>
              <![CDATA[
             <table ..> ...
                 <td ...">Name</td>
                 <td ...">john doe</td>
                 ..
                  ..</table> ]]>
    </update> ...
</partial-response>
```

Figure 6: Composite payload masking example

These steps are realized using the following processors and selectors

1. An XML processor that parses XML payloads, support XPath Syntax expressions to select XML nodes and support updating of selected nodes.
2. A HMTL processor that parses HTML payload, support CSS Syntax and selectors as well as support updating of selected elements.
3. A Masking Processor which is able to mask text, e.g. replace text with '*',
4. An XPath selector that specifies the relevant XPath, and
5. A CSS selector that specifies the relevant CSS path.

A graph connecting the described processors and selector is shown in the following figure 7.

Figure 7: Masking engine instance example

The hiding tool main interface is a single method called process. This method receives the payload, policy and a few more additional arguments and provides as a result the processed payload (e.g. masked/unmasked).

How does the Data Sensitivity work?

The process of identifying sensitive data is a necessary step to be able to address EU GDPR regulation. The first step is to discover the personal data in the organization datastores, categorize the data, and finally apply appropriate methods to protect the data. Given a category, the organization can adhere to a specific GDPR requirement. For example, the GDPR defines special categories such as racial and health data. A company must have a legitimate and lawful reason for collecting, storing, transmitting, or processing these special categories.

The Data Sensitivity Analysis Tool addresses the first step. It finds the sensitive/personal data in relational databases. The tool is provided with DB tables for analysis and a configuration. The configuration allows us to customize the tool and select relevant predefined classifiers. In addition, the tool provides the ability to define custom classifiers. The tool analyses each one of the tables and provides the table categories as well as specific information for each column. This information includes the column categories and sub-categories, each attached with a corresponding confidence score.

Internally, the tool utilizes several methods to identify categories. These include simple methods – "single value classifiers" - such as regular expression, dictionaries as well as methods to check complex restrictions such as Luhn checksum. Instead, the tool uses advanced statistical analysis and it is able to account for multiple values in the column to differentiate between categories which may have overlapping values.

Specifically, this is accomplished by applying different types of statistics which can differentiate correctly between the categories. The next figure 8 shows one type of statistic able to differentiate between categories based on the distance of the discrete distribution of the sample from the one expected for each category.

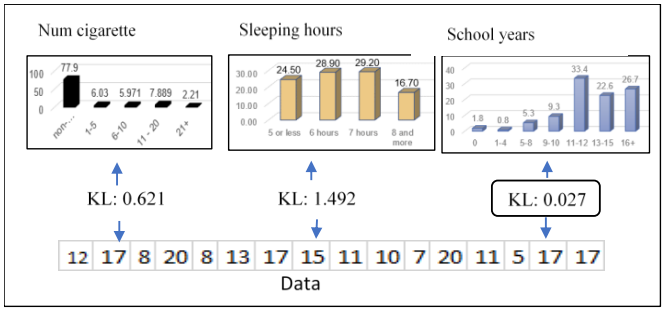

Figure 8: Applying Kullback-Leibler distance on discrete distribution [Assaf et al., 2019]

4 Case study

4.1 General overview

Our case study is based on the following situation [Larrucea et al., 2020], where a UK citizen travelling to Spain incurs a stroke, he/she is taken to the nearest Spanish hospital, and medical doctors ask for his/her patient's electronic health records (EHR). Each country has its own NHS, and there is an exchange of data between hospitals.

4.2 Business Processes Layer

This layer deals with the consent management in a healthcare industry 4.0 context where 2 different countries must collaborate and share patient's health records for assisting a patient travelling from one country to another.

This case study is also based on the case studies reflected in [Larrucea et al., 2019] where they use the same situation as a testing example. In this case, a UK citizen travelling to Spain incurs a stroke and is taken to the nearest Spanish hospital. While receiving first aid from the Emergency Medical Services (EMS), the coordination centre informs the EMS in which hospital the patient should be taken to. At the same time a message is sent to a workstation located in the emergency department of the hospital responsible for alerting the first-aid unit. As soon as the message is received a medical team is created for the stroke assistance. To ensure the best assistance, the medical staff wishes to check the patient's electronic health records (EHR) to know their medical history (e.g. their epSOS patient summary).

From a technical point of view, Figure 9 represents the solution where different National Health Systems are interconnected ['Smart Open Services for European Patients', 2018]. Figure 9 includes the two members of the European Union that are connected by using OpenNCP. Each national OpenNCP installation plays a relevant role within the consent management. This business process involves different OpenNCP nodes and each node includes a set of functionalities in order to strength data security and privacy. Security is a chain and it is as strong as its weakest link and all these NHSs are connected by using this platform.

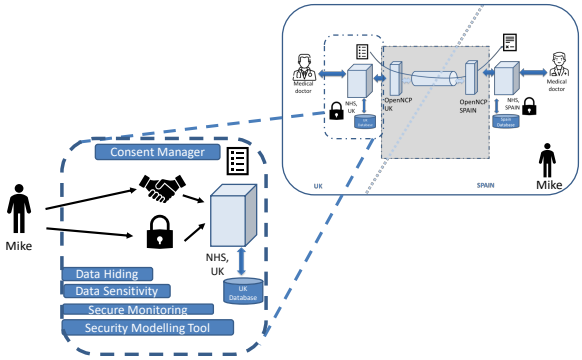

Figure 9: Reference Architectural Model Industry 4.0 adopted for the healthcare industry 4.0

Each national contact point has the same set of tools for managing consent, for hiding sensitive data, and for secure monitoring (Figure 9).

Data Layer

As this layer is central aspect of our resulting platform, we show in Figure 10 the main UI for data hiding tool. The UI allows the user to create, manage and test the hiding policies. Note, during runtime the data hiding tools' 'process' API is called with the policy id and relevant payload.

Obviously, there are several connections between different tools such as the consent manager, the data hiding tool and the extended OpenNCP, but we just want to highlight the tool we have developed and used for supporting the approach.

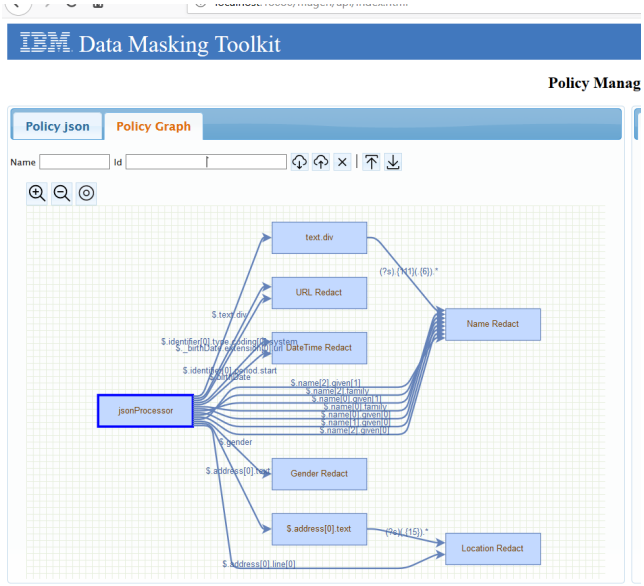

Figure 10: Data Masking toolkit, policy graph

Figure 10 shows the policy graph (data flow) created to mask the sensitive data in the patient health record. In the following paragraphs we provide an example of the outcomes of this tool.

Example of an eHealth record masked

The data hiding tool was used to hide specific data in a Psychiatry Discharge Report (XML based) and was configured to account for the consent provided by the user and hide only the non-consented information.
Figure 12 shows a XML example of a clinical document before being processed, and it shows the result after the masking tool was invoked. In this case, as a result all attributes are encrypted based on the consent.

```
<?xml version="1.0" encoding="UTF-8"?>
<ClinicalDocument xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:voc="urn:hl7-org:v3/voc"                    xmlns="urn:hl7-org:v3"
xsi:schemaLocation="urn:hl7-org:v3 CDASchema/CDA.xsd">
...
      <component>
        <section>
          <templateId            root="2.16.840.1.113883.10.20.22.2.15"
extension="20170509"/>
          <code code="10157-6" codeSystem="2.16.840.1.113883.6.1"/>
          <title>ANTECEDENTES FAMILIARES</title>
          <text>
            <paragraph>Madre con antecedentes de depresión que requisó
ingreso hospitalario. Tío materno con esquizofrenia. Tía materna con
depresión</paragraph>
          </text>
        </section>
      </component>
      <component>
...
```

Figure 11: An example of the XML unmasked

```
<?xml version="1.0" encoding="UTF-8"?>
<ClinicalDocument xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:voc="urn:hl7-org:v3/voc"                    xmlns="urn:hl7-org:v3"
xsi:schemaLocation="urn:hl7-org:v3 CDASchema/CDA.xsd">
...
      <component>
        <section>
          <templateId              extension="6Caf3Sqq11IWkLHcvAH/yg=="
root="oRssaWwwV45ZoqEv571KUR27AGBh8vzl2VtOMjiyJI0="/>
          <code                          code="phntHMAorf0xd0ujEZStmw=="
codeSystem="oRssaWwwV45ZoqEv571KUXq8zpTGZhb8iuiNIR7NS+k="/>
<title>ZiUWkE3R8pE7gyaLyIvQT1KC62AHvAxaZBHahow7sio=</title>
<text>
<paragraph>Oe4K6ocNFUyc6xafXTT6Ipl9yci4IcYzmDJrxlonGo3XJ+cPNXISv9jZyQH
57ijqSd5KO0KoWQYqez+wFCVKr5xFPDecKEDv7vtSA30wp4VeG7ZVcsj7KXbqxqbDQF6Je
7UjCU/uOD4epWG0KthZeXaUmoQC2htjl3IEGhTPt8M=</paragraph>
          </text>
        </section>
      </component>
...
```

Figure 12: An example of the XML masked

Example of a Data Sensitivity work

We run the Data Sensitivity Analysis tool on consultation table with our case study NHS DB. This table contains patient info including many Direct and Indirect (Quasi) Personal Identifier information such as name, phone, national id and birth date. The purpose was to categorize correctly each of the table columns. The tool found that the table contains both Direct and Indirect (Quasi) Personal Identifiers. In addition, for each column it provides its category and subcategories.

Figure 13 displays part of the JSON result for the consultation table. As illustrated, the consultation table contains both Direct Identifier and Quasi Identifier columns. The HCP_ID column is identified as a Quasi Identifier and the results show a high likelyhood (confidence score of 0.9) that it contains sensitive information.

```
"tables": {
  "name": "consultation",
  "categories": [
  { "category": "Direct Identifier",
    "score": 1.0},
  { "category": "Quasi Identifier",
   "score":             1.0             }],

"columns": [
{ "name": "HCP_ID",
  "category": {
     "category":"Quasi Identifier",
     "score":0.9},
   "subCategories": [
    { "category": "Region",
      "score": 0.9 }]
} …
```

Figure 13: JSON result for the consultation table

5 Conclusions

The GDPR is being considered as a fundamental requirement in any software system managing or processing personal information. Our industry 4.0 architecture and our set of tools such as consent management, data sensitivity and data hiding tools are key elements for fulfilling with GDPR requirements. These articles are the followings:

- "Article 5. Principles relating to processing of personal data". In fact, the medical records exchanged are collected for specified, explicit and legitimate purposes
- "Article 6 Lawfulness of processing". In our solution patients have given consent to the processing of his or her personal data for one or more specific purposes. In addition, our data hiding tools are considered as appropriate safeguards, which include encryption or pseudonymisation
- "Article 7 Conditions for consent". As we are using a consent management tool, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
- "Article 8 Conditions applicable to child's consent in relation to information society services". This is a special case which can be tackled with our solution.
- "Article 9 Processing of special categories of personal data". This is the case for medical records.

The use of our approach is a step forward for the current development of the OpenNCP platform. We are providing a way to enhance security and privacy between different NHS from different countries, and to enhance compliance to GDPR processing and managing patients' data. We have defined and used consent manager and the data hiding tool for sharing health records, and we have used a healthcare industry 4.0 reference framework.

Our case study illustrates some of the real-world complexities and how the approach we took can address those complexities. This includes identifying and categorizing the information that is subject to GDPR and consent, integrating the consent manager and data hiding tool within the data flow while providing the user fine grained control over his personal data.

As a future work, we are working on the exchange of patients' data originating from mobile devices, and on how to integrate them into NHS, and on how to prevent data breaches within this complex scenario.

6 References

[Alloghani et al., 2018] Alloghani, M., Al-Jumeily, D., Hussain, A., Aljaaf, A. J., Mustafina, J., Petrov, E.: 'Healthcare Services Innovations Based on the State of the Art Technology Trend Industry 4.0'; In 2018 11th International Conference on Developments in eSystems Engineering (DeSE). Cambridge, United Kingdom: IEEE (2018), 64–70. https://doi.org/10.1109/DeSE.2018.00016

[Asghar et al., 2017] Asghar, M. R., Lee, T., Baig, M. M., Ullah, E., Russello, G., Dobbie, G.: 'A Review of Privacy and Consent Management in Healthcare: A Focus on Emerging Data Sources'; IEEE (2017), 518–522. https://doi.org/10.1109/eScience.2017.84

[Assaf et al., 2019] Assaf, S., Farkash, A., Moffie, M.: 'Multi-value Classification of Ambiguous Personal Data'; In C. Attiogbé, F. Ferrarotti & S. Maabout (Eds.), New Trends in Model and Data Engineering (Vol. 1085). Cham: Springer International Publishing (2019), 202–208. https://doi.org/10.1007/978-3-030-32213-7_16

[Badri et al., 2018] Badri, A., Boudreau-Trudel, B., Souissi, A. S.: 'Occupational health and safety in the industry 4.0 era: A cause for major concern?'; Safety Science, 109 (2018), 403–411. https://doi.org/10.1016/j.ssci.2018.06.012

[Buchanan et al., 2013] Buchanan, W. J., Uthmani, O., Fan, L., Burns, N., Lo, O., Lawson, A., et al.: 'Modelling of Integrated Trust, Governance and Access'; In M. Felici (Ed.), Cyber Security and Privacy (Vol. 182). Berlin, Heidelberg: Springer Berlin Heidelberg (2013), 91–101. https://doi.org/10.1007/978-3-642-41205-9_8

[Celesti et al., 2019] Celesti, A., Amft, O., Villari, M.: 'Guest Editorial Special Section on Cloud Computing, Edge Computing, Internet of Things, and Big Data Analytics Applications for Healthcare Industry 4.0'; IEEE Transactions on Industrial Informatics, 15, 1 (2019), 454–456. https://doi.org/10.1109/TII.2018.2883315

[Conley and Pocs, 2018] Conley, E., Pocs, M.: 'GDPR Compliance Challenges for Interoperable Health Information Exchanges (HIEs) and Trustworthy Research Environments (TREs)'; European Journal for Biomedical Informatics, 14, 3 (2018), 48–61.

[David et al., 2014] David, M., Rosa, F., Rodrigues, P. P.: 'Need and Requirements Elicitation for Electronic Access to Patient's Medication History in the Emergency Department'; IEEE (2014), 497–498. https://doi.org/10.1109/CBMS.2014.108

[EHDEN consortium, 2020] EHDEN consortium: 'European Health Data & Evidence Network (EHDEN)'; (2020). Retrieved from https://www.ehden.eu/

[Elhoseny et al., 2018] Elhoseny, M., Abdelaziz, A., Salama, A. S., Riad, A. M., Muhammad, K., Sangaiah, A. K.: 'A hybrid model of Internet of Things and cloud computing to manage big data in health services applications'; Future Generation Computer Systems, 86 (2018), 1383–1394. https://doi.org/10.1016/j.future.2018.03.005

[European Commission, n.d.-a] European Commission: 'eHealth DSI Operations'; (n.d.-a). Retrieved from https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHealth+DSI+Operations+Home

[European Commission, n.d.-b] European Commission: 'OpenNCP'; (n.d.-b). Retrieved from https://ec.europa.eu/cefdigital/wiki/display/EHNCP

[Hathaliya et al., 2019] Hathaliya, J. J., Tanwar, S., Tyagi, S., Kumar, N.: 'Securing electronics healthcare records in Healthcare 4.0 : A biometric-based approach'; Computers & Electrical Engineering, 76 (2019), 398–410. https://doi.org/10.1016/j.compeleceng.2019.04.017

[Health information Institute, 2010] Health information Institute: 'NHS Electronic Health Record System'; (2010). Retrieved from http://www.mscbs.gob.es/en/organizacion/sns/planCalidadSNS/docs/HCDSNS_English.pdf

[Heinze et al., 2011] Heinze, O., Birkle, M., Köster, L., Bergh, B.: 'Architecture of a consent management suite and integration into IHE-based regional health information networks'; BMC Medical Informatics and Decision Making, 11, 1 (2011). https://doi.org/10.1186/1472-6947-11-58

[Javaid and Haleem, 2019] Javaid, M., Haleem, A.: 'Industry 4.0 applications in medical field: A brief review'; Current Medicine Research and Practice (2019). https://doi.org/10.1016/j.cmrp.2019.04.001

[Karat et al., 2009] Karat, J., Karat, C.-M., Bertino, E., Li, N., Ni, Q., Brodie, C., et al.: 'Policy framework for security and privacy management'; IBM Journal of Research and Development, 53, 2 (2009), 4:1-4:14. https://doi.org/10.1147/JRD.2009.5429046

[Larrucea et al., 2020] Larrucea, X., Moffie, M., Asaf, S., Santamaria, I.: 'Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0'; Computer Standards & Interfaces, 69 (2020), 103408. https://doi.org/10.1016/j.csi.2019.103408

[Larrucea et al., 2019] Larrucea, X., Santamaria, I., Colomo-Palacios, R.: 'Assessing source code vulnerabilities in a cloud-based system for health systems: OpenNCP'; IET Software, 13, 3 (2019), 195–202. https://doi.org/10.1049/iet-sen.2018.5294

[Lezzi et al., 2018] Lezzi, M., Lazoi, M., Corallo, A.: 'Cybersecurity for Industry 4.0 in the current literature: A reference framework'; Computers in Industry, 103 (2018), 97–110. https://doi.org/10.1016/j.compind.2018.09.004

[Pace et al., 2019] Pace, P., Aloi, G., Gravina, R., Caliciuri, G., Fortino, G., Liotta, A.: 'An Edge-Based Architecture to Support Efficient Applications for Healthcare Industry 4.0'; IEEE Transactions on Industrial Informatics, 15, 1 (2019), 481–489. https://doi.org/10.1109/TII.2018.2843169

[Pang et al., 2018] Pang, Z., Yang, G., Khedri, R., Zhang, Y.-T.: 'Introduction to the Special Section: Convergence of Automation Technology, Biomedical Engineering, and Health Informatics Toward the Healthcare 4.0'; IEEE Reviews in Biomedical Engineering, 11 (2018), 249–259. https://doi.org/10.1109/RBME.2018.2848518

[Pfeiffer, 2017] Pfeiffer, S.: 'The Vision of 'Industrie 4.0' in the Making—a Case of Future Told, Tamed, and Traded'; NanoEthics, 11, 1 (2017), 107–121. https://doi.org/10.1007/s11569-016-0280-3

[Pocs, 2012] Pocs, M.: 'Will the European Commission be able to standardise legal technology design without a legal method?'; Computer Law & Security Review, 28, 6 (2012), 641–650. https://doi.org/10.1016/j.clsr.2012.09.008

[Rios et al., 2019] Rios, E., Iturbe, E., Larrucea, X., Rak, M., Mallouli, W., Dominiak, J., et al.: 'Service level agreement-based GDPR compliance and security assurance in (multi)Cloud-based systems'; IET Software (2019). https://doi.org/10.1049/iet-sen.2018.5293

[Russello et al., 2008] Russello, G., Dong, C., Dulay, N.: 'Consent-Based Workflows for Healthcare Management'; IEEE (2008), 153–161. https://doi.org/10.1109/POLICY.2008.22

[Schweichhart, 2016] Schweichhart, K.: 'Reference Architectural Model Industrie 4.0 (RAMI 4.0)'; (2016). Retrieved from https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf

[Shapiro et al., 2016] Shapiro, J. S., Crowley, D., Hoxhaj, S., Langabeer, J., Panik, B., Taylor, T. B., et al.: 'Health Information Exchange in Emergency Medicine'; Annals of Emergency Medicine, 67, 2 (2016), 216–226. https://doi.org/10.1016/j.annemergmed.2015.06.018

[SHiELD project, 2017] SHiELD project: 'Deliverable D5.8 Consent Management'; (2017). Retrieved from https://project-shield.eu/Content/PDFs/D5.8.pdf

['Smart Open Services for European Patients', 2018] (2018). Retrieved from https://www.itu.int/net4/wsis/stocktaking/projects/Project/Details?projectId=1399467257

[Staffa et al., 2018] Staffa, M., Sgaglione, L., Mazzeo, G., Coppolino, L., D'Antonio, S., Romano, L., et al.: 'An OpenNCP-based Solution for Secure eHealth Data Exchange'; Journal of Network and Computer Applications, 116 (2018), 65–85. https://doi.org/10.1016/j.jnca.2018.05.012

['Symphonic', 2020] (2020). Retrieved from https://www.symphonicsoft.com/

[The European Parliament And Of The Council, 2016] The European Parliament And Of The Council: 'Directive 95/46/EC (General Data Protection Regulation)'; Official Journal of the European Union (2016, April 27). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[The European Parliament And The Council Of The European Union, 2011] The European Parliament And The Council Of The European Union: 'Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare'; (2011, September 5). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024

[Weber-Jahnke and Obry, 2012] Weber-Jahnke, J. H., Obry, C.: 'Protecting privacy during peer-to-peer exchange of medical documents'; Information Systems Frontiers, 14, 1 (2012), 87–104. https://doi.org/10.1007/s10796-011-9304-2

[Wismar et al., 2011] Wismar, M., Palm, W., Figueras, J., Ernst, K., van Ginneken, E.: 'Cross-border Health Care in the European Union: Mapping and analysing practices and policies'; (2011). Retrieved from http://www.euro.who.int/__data/assets/pdf_file/0004/135994/e94875.pdf