Ensuring Secure Health Data Exchange across Europe. SHIELD Project

Borja López-Moreno[1], David Martín-Barrios[2], Ivan Revuelta-Antizar[1], Santiago Rodríguez-Tejedor[3], M. Luz del Valle[1] and Eunate Arana-Arri[1]

[1]Biocruces Bizkaia Health Research Institute, Plaza Cruces 12, Barakaldo, Spain
[2]Ibermatica, Derio, Parque Tecnológico de Bizkaia Ed. 501A, Spain
[3]Cruces University Hospital, Osakidetza, Plaza Cruces 12, Barakaldo, Spain

Keywords: Secure Health Information Exchange, General Data Protection Regulation, e-Consent, Electronic Medical Records, Patient Summaries, eHealth Interoperability.

Abstract: Nowadays, many people move from one country to another for various reasons: tourism, work, studies, etc.; even with chronic or multi-pathological diseases. The main objective of SHIELD project is to create open and extendable security architecture with supported privacy mechanisms and trust of citizens, to provide systematic protection for the storage and exchange of health data across European borders. epSOS is a European project funded and finished dealing with security and interoperability of eHealth data is, that result in an OpenNCP (National Contact Point) architecture. In SHIELD project for the initial validation framework two OpenNCP virtual nodes would simulate the real nodes between Italy and Spain. Validation scenarios (realistic use cases) have been developed in three different member states (Italy, United Kingdom and Spain). The first scenario is an Italian citizen traveling to Spain that has an acute emergency episode (e.g. stroke) and loses consciousness. Spanish emergency department suddenly assists that patient and doctor wishes to check patient´s health record. Results of the first round of validation frameworks of SHiELD project have been made successfully and presented to the European Commission. Security challenges need to be addressed when assessing eHealth solutions. Among others, the challenges are: interoperability, confidentiality, availability, integrity, privacy, ethics, regulations and eHealth data. Which data are going to be shared and by which mean? The first validations will be useful as the basis for both the "in depth" requirements analysis as well as setting the main pillars for the SHIELD architecture detailed design.

1 INTRODUCTION

The development of new eHealth tools and the implementation of new policies in the European Union (EU) can help to guarantee more efficient and sustainable health services, and with this increase the safety in the management of patients. In addition, all this guarantees a better communication between different professionals, end-users and other decision makers. In the first e-Health Action Plan of the European Commission (EC) (2004) these benefits were fully recognized. Since then, the Commission has made an important effort to promote and develop specific political actions in this context (European Commission, 2011; European Commission, 2012).

Security is one of the main challenges when applied to eHealth and is crucial in the transmission of required data about patients and citizens when traveling around the world.. Thus, there is a growing need of rapid and secure access to clinical data between different healthcare systems, at the national and international levels.

The potential value of health data is huge, both in traditional health sectors (e.g. for medical research such as drug design) and in new sectors, such as personalised health and lifestyle management services based on wearable devices. Recent estimates indicate that person's health data is 50 times more valuable than their financial data (Minor, 2017). Unfortunately, health data is not only valued highly by potential legitimate users. Cyber criminals also regard health data as between 20 and 50 times

López-Moreno, B., Martín-Barrios, D., Revuelta-Antizar, I., Rodríguez-Tejedor, S., Valle, M. and Arana-Arri, E.
Ensuring Secure Health Data Exchange across Europe. SHIELD Project.
DOI: 10.5220/0007524004220430
In *Proceedings of the 12th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2019)*, pages 422-430
ISBN: 978-989-758-353-7

more valuable than financial data, mainly because it allows them to create very convincing false identities based on individual personal histories (Luna, 2016). Stealing credit card details provides only a limited window of opportunity for criminals before the card is cancelled by its rightful owner. However, health records cannot be cancelled, and provide criminals with opportunities for identity theft over a long period. There are also dangers from the use of health data by legitimate businesses.

That is why another of the great challenges is to comply with the General Data Protection Regulation (EU) 2016/679 (EU, 2016) also known as GDPR on processing of personal data and on the free movement of such data (Pocs, 2012).

The main objective of the SHIELD project is to create an open and extendable security architecture supported on security and privacy mechanisms to provide systematic protection for the storage an exchange of health data across European borders, while improving patients trust in the security of their data.

2 METHODS

The exchange of health data is already possible, but rarely happens in practice because it is hard to ensure that the combined 'end-to-end' system will be secure and comply with data protection laws. SHiELD will address these security and compliance challenges:

- providing models and analysis tools for automated identification of end-to-end security risks and compliance issues and supporting privacy 'by design';
- defining an open and extensible data exchange architecture based on epSOS (epSOS, 2012), able to support security measures to address these risks;
- developing security mechanisms to deal with new and emerging risks, such as inference attacks on sensitive data, and risks from relatively unprotected mobile edge devices;
- providing faster and more cost-effective methods to verify and monitor compliance with multiple sets of applicable regulations.

SHiELD aims address security and regulatory compliance challenges in two distinct situations:

- where a business needs access to health data to develop or operate a high value health or lifestyle related product or service, including wearable devices and associated services;
- when a citizen´s health care is needed in one Member State, and care givers need access to their health (or lifestyle) data which may be stored in a different Member State.

The validation case studies are designed to cover both these situations, both separately and in combination.

SHiELD case studies will address cross border scenarios in which a citizen needs health care while in one Member State, and care givers need access to their health data from different Member State. SHiELD will also consider how commercial providers of lifestyle services or wearable sensors may be involved in such data exchanges. SHiELD will thereby also create opportunities for using health data to create such products and services addressing the common European market. SHiELD will provide guidance in best practice to achieve end-to-end security and data protection compliance in health and health related applications.

2.1 Pilot Case Studies

Validation scenarios (realistic use cases) have been developed in three different member states (Italy, United Kingdom and Spain). In all scenarios, we assume that a citizen travels abroad and needs health care. The foreign health care professional needs to access and/or manage patient's health record. Results of the first round of validation frameworks of the SHiELD project have been made successfully and presented to the European Commission.

Three use cases have been prepared with different characteristics. Different levels of need for attention have been developed: a case in which the patient can't consent because he or she is unconscious, but it is a vital emergency; another case in which the patient consents to what information he wants to share and the third case, requires exchange between more than two countries and also adds data from devices provided by the patient.

2.1.1 Use Case 1: "Break Glass" Circumstance

An Italian citizen travelling in Spain incurs a stroke and is taken to the nearest Spanish hospital. While receiving first aid from the Emergency medical services (EMS), the coordination center 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.

For this purpose, different physicians are summoned: emergency physicians, neurologist. neuroradiologist and anaesthesiologist.

In order to ensure the best assistance, the medical staff wishes to check the patient's Electronic Health Record (EHR) to know their medical history (e.g. their epSOS patient summary). Since the patient is foreign, this is possible thanks to the SHiELD platform, which ensures the communication between NCPs of different countries within Europe in a secured manner.

This is fundamental, not only to discover possible illnesses or chronic conditions, but also to ensure that the patient does not suffer from allergies to drugs; also if the patient receives treatment for a chronic condition, that should be relevant in order to be able to perform a therapeutic management as efficiently as possible.

Indeed, the first aid protocol for a stroke may vary in case of other pathologies or allergies. For example, in case of renal failure the cranium computed tomography scan (the traditional examination in case of stroke) can be replaced with an magnetic resonance imaging in order to avoid contrast agent, which can aggravate kidney conditions. The fibrinolytic treatment has shown an important reduction in mortality and morbidity in patients with stroke, but all treatments may have contraindications when applied, and it is so important to know about them in order to not generate iatrogenic damage in the patient. Examples for such contraindications are oral anticoagulant treatment, recent history of severe bleeding, severe liver disease, hemorrhagic retinopathy, etc.

It could be possible that the patients receive endovascular treatment. This case needs general anesthesia in an operating room, and having access to patient´s EHR for the anesthesiologist could be vital.

This is just to demonstrate the importance of the patient clinical history; the epSOS clinical record summary with the mandatory basic dataset will be enough to perform an appropriate management at the time of the incident. It could be possible to extend this information to other examinations (e.g. blood tests, bio images etc.) made in the 60 days preceding the "break glass" circumstance, that are usually sufficient to give a general overview of the clinical condition. This means that the chance of patient survival increases if the physician has access to the patient's clinical record as quickly as possible. Consequently, a better patient response is expected, the faster the therapy is provided. In the management of stroke in the emergency services there is a saying that "time is brain".

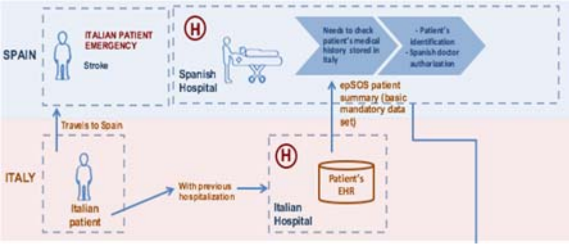

SPAIN
ITALIAN PATIENT EMERGENCY
Stroke
Spanish Hospital
Needs to check patient's medical history stored in Italy
- Patient's identification
- Spanish doctor authorization
epSOS patient summary (basic mandatory data set)
Travels to Spain
ITALY
Italian patient
With previous hospitalization
Patient's EHR
Italian Hospital

Figure 1: Use Case 1 graph.

2.1.2 Use Case 2: Surgical Intervention

A Spanish patient has had a surgical intervention (e.g. urological surgery) and he is planning to travel across the EU within two months of the surgery.

The patient wants to have details of the surgical intervention at his disposal in case it is needed for medical assistance during the travel abroad. At this scope the patient, together with the Italian urological surgeon, decides - using the mobile interface of the "SHiELD" platform - which information would be useful to share with a foreign doctor during the trip. They decide to share part of the hospital discharge letter, including detailed information about the patient's clinical history and the recent surgery. The SHiELD solution will also give the possibility to hide sensitive information capturing patient consent.

Moreover, the patient, using the "SHiELD platform", can make the decision, relevant for privacy issues, of when and where to share this information. This is meant to limit the availability of the shared information in time and location (e.g. "in Milan for the next 2 weeks"). Access preferences will be integrated into the access model to ensure the balanced concerns of patient privacy and treatment need.

In case of post-surgical complications during the trip, after providing first aid, the emergency physicians must have access to the EHR, including the most recent clinical and surgical steps.

Initially, the doctor has access to the epSOS Patient Summary with basic information, in order to discover the type of surgical procedure performed; then, they want to access detailed information about the surgical procedure itself, all the complementary tests carried out in the process, and therefore decide to visualise the extract of the discharge letter shared by the patient.

The patient and his doctor agree on the contents to be shared on the platform, in order to be available to a third party, (e.g. a foreign medical professional).

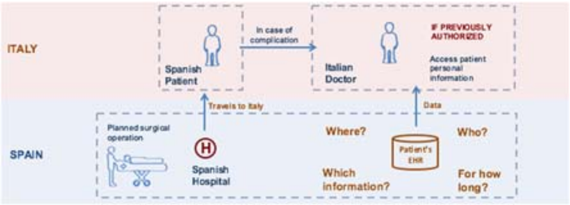


Figure 2: Use Case 2 graph.

2.1.3 Use Case 3: Chronic Conditions + Remote Monitoring

A 40 year old Italian woman with type 1 diabetes mellitus under treatment with insulin stays in the UK for work reasons for 3 month. She's been living in the Basque country for 10 years. The woman, prior to her stay in the UK, gives consent to access her medical history. In the Basque Health System the EHR has the Health Folder. By the Health Folder the patient can send and receive information from and to her General Practitioner (GP). The patient will use this resource to monitor her pre-prandial glycaemia, as prescribed by her GP. During her stay in the UK, she has agreed with her GP that, since this is another country, she will record her eating habits as well as her physical activity. She will send this information by the Health Folder.

After a week in the UK, she begins to notice dizziness accompanied by general discomfort and sometimes nausea. As it does not happen every day and the glycaemia is within normal range, she decides to take care of her diet and continue with her usual treatment schedule. She blames these episodes on the stress caused by her new job. After several days without any improvement of her symptoms, being at work she presents a transient loss of consciousness (syncope) with a fall to the ground and a slight traumatic brain injury, with total recovery of consciousness. Her colleagues decide to take her to the nearest hospital emergency department.

During the patient's anamnesis, she refers to a brain surgery she had as a child in Italy, but she does not know any details. This old episode could be of great importance for the management of the incident.

As in the other cases, in order to ensure the best assistance, the medical staff wish to check the patient's EHR to access her medical history (e.g. her epSOS patient summary), but in this scenario, the accessibility to more than the patient summary could be helpful for the medical staff. Since the patient is foreign, this is possible thanks to the SHiELD platform, which ensures the communications between NCPs of different countries within Europe.

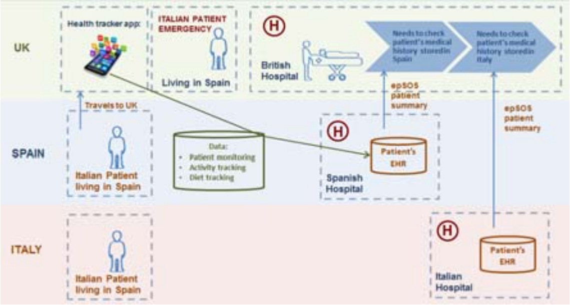


Figure 3: Use Case 3 graph.

2.2 Definition of Work Packages (WP)

In order to respond the multidisciplinary and interrelated proposed approach, SHiELD proposes a work plan covering all particular project aspects (legal, security, privacy), considering the relationship among all these aspects. The work is divided into 7 work packages. Figure 4 shows the complete picture of work packages.

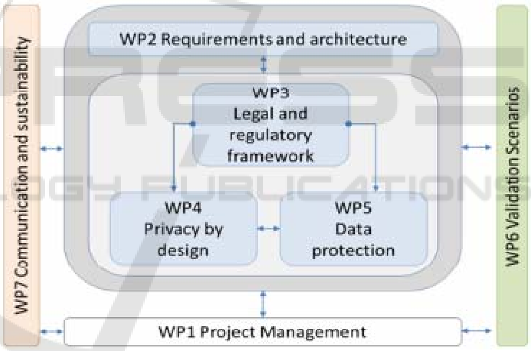

WP2 Requirements and architecture
WP3 Legal and regulatory framework
WP4 Privacy by design
WP5 Data protection
WP1 Project Management
WP7 Communication and sustainability
WP6 Validation Scenarios

Figure 4: Work packages relation.

WP1 consists in Project management and WP7 deals with Communication and sustainability, WP3 Legal and regulatory framework, so this document focus on the work packages WP2, WP4, WP5 and WP6.

2.2.1 WP2 – Requirements and Architecture

The main objectives for this work package are to design the overall architecture of SHiELD and to design and continuously integrate the SHiELD tool following an iterative, continuous integration and continuous deployment in order to smoothly integrate the different tools to be developed within SHiELD.

The main result of this WP will be the SHiELD architecture that will be validated in the case studies defined in this project, as well as the open architecture and secure interoperability API.

2.2.2 WP4 – Privacy by Design

The objectives of this work package are to develop models capturing potential threats to health data, to develop models capturing health data protection regulatory compliance requirements in at least three European jurisdictions, to devise architectural design patterns that are secure with respect to threats and address regulatory compliance requirements and to develop software tools that can use these models and design patterns to automatically analyses the end-to end security of health data and compliance requirements for specific systems.

2.2.3 WP5 – Data Protection

The objectives of this work package are to develop data protection mechanisms and tools, to develop privacy protection mechanisms and tools, to incorporate developed mechanisms and tools within the SHiELD architecture and to address regulatory compliance requirements.

2.2.4 WP6 – Validation Scenarios

This Work Package targets the definition of a solid methodology for the scientific, technical and legal validation of the tools and prototypes developed in the project. The challenges are to define realistic use cases identifying real-life-strength scenarios, to define suitable metrics and protocols supporting a solid validation framework, to identify relevant use cases for the scenarios of the project, to implement the use cases and to evaluate the integration and interoperability level of the architecture with other tools.

3 RESULTS

One of the European projects funded and already finished dealing with the security and interoperability of eHealth data is epSOS project that result in an OpenNCP (National Contact Point) architecture and implementation. The OpenNCP community has designed and developed a set of Open Source Components based on the services developed in epSOS. This can be used by Participating Nations to build their local implementation of an NCP. However, this has not been validated and put into practice (epSOS, 2012).

In SHIELD project for the initial validation framework experiments two OpenNCP virtual nodes would simulate the real nodes between Italy and Spain (Virtual Machines). For the secure exchange of clinical health records different prototype tools have been designed and are being developed: end-to-end user interfaces for different health systems profiles (administrative staff, nurses, physicians, etc.), sensitivity tools, data hiding tools, consent management tools, reports translation tools and mobile devices tampering detection tools.

One of the main achievements to be fulfilled in SHIELD is the end-to end systemic analysis of potential risks to health data. This is being performed by creating a knowledge base from potential threats including ´classical´ cyber security threats, emerging threats to personal data and compliance threats. SHIELD will unlock the value of health data to European citizens and other stakeholders by overcoming security and regulatory challenges that today prevent this data being exchanged with those who need it, especially in emergency situations.

3.1 Validation of WP2

3.1.2 Description of the OpenNCP Architecture and Clinical Data Interchange

In the initial validation experiments two OpenNCP nodes would simulate the real nodes between Italy and Spain. This deployment would fit the first Use Case scenario.

The minimal infrastructure needed to simulate it, are (Figure 5) (HL7, 2012):

- Spanish OpenNCP Node:
    - (Virtual Machine) Ubuntu Server 16.06 simulating Spanish OpenNCP Node.
    - (Virtual Machine) Basque Health service (that would implement the underlying communication with the central patient database on the Spanish side.
    - (Virtual Machine) Ubuntu Server 16.06 simulating Italian OpenNCP Node (Italian data underlying patient database are simulated in this virtual machine).
- Both OpenNCP nodes are Linux distributions that contains some features to host the OpenNCP core like: Mysql databases, Apache Tomcat and JDK 1.8.

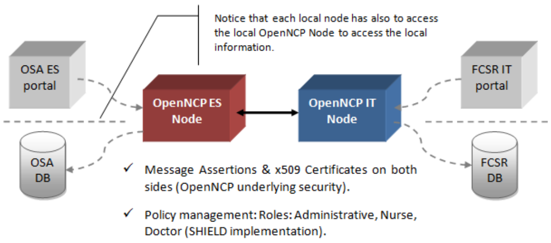
OpenNCP should be able to:

- Communicate with their own services through OpenNCP local node.

- Communicate with a remote node (from the Spanish OpenNCP to the Italian OpenNCP).
- Communcation backwards: communicate with a source remote node (from the Italian OpenNCP to the Spanish OpenNCP).

Clinical Document Architecture (CDA) has been used to markup standard that specifies the structure and semantics of "clinical documents" for the purpose of exchange between healthcare providers and patients (eHealth DSI Semantic Community. 2012, Boone, 2012). For the simulation of sending clinical data between OpenNCP nodes, is needed the creation of a fake patient with useful clinical data for the Use Case, with its correct structure (XML HL7 CDA Level 3). The format of the Patient Summary must be HL7, CDA Level 3: in the case of Osabide Global (Basque Health service´s EHR) and unlike other reports, CDA level 3 (HL7) will be required, which indicates that both the header and the body will be properly structured. That is, just as other reports will be sent embedded in Portable Document Format (PDF), in the case of Osabide Global, the XML should be sent properly structured according to the standard HL7 CDA level 3 coding.

As described before, the Basque Health service’s web portal will provide the access OpenNCP endpoints to lookup for patients on their origin countries. It is the Doctor who will access to the patient summary and who will obtain critical information of the patient, like the past illness history, the medication section or the allergies. Moreover, in this implementation the doctor would be also able to obtain other associated clinical documents, like laboratory results, electro-cardiogram or echocardiogram from the Spanish patient. The Italian side would also provide laboratory results as other associated documents.



Notice that each local node has also to access the local OpenNCP Node to access the local information.

✓ Message Assertions & x509 Certificates on both sides (OpenNCP underlying security).

✓ Policy management: Roles: Administrative, Nurse, Doctor (SHIELD implementation).

Figure 5: OpenNCP nodes implemented in virtual machines.

3.2 Validation of WP4

This work package is divided in two subsections:

- *Security Modelling Tools:* creates design-time (“offline”) modelling tools to support the modelling of health data being transferred as required by the use cases described, later, in WP6. This report describes the existing tool including some generic improvements and initial versions of the extensions to support modelling of regulatory compliance.

Here, it uses the “System Modeller” tool that enables the user to create design-time models of IT systems describing healthcare applications. Additionally, to basic functionality such as signing in and out, performing CRUD (Create, Read, Update, Delete) operations on models and import/export of models, it supports: validating a model, i.e. generating a threat catalogue by matching pre-defined patterns from the knowledge base in the system asserting controls directly on assets or applying control strategies to block threats accepting threats, for example when they don’t have a control strategy System Modeller relies on the security knowledge base in order to perform any of these tasks.

- *Security Knowledge Base:* captures potential security and compliance threats in a knowledge base. The initial threats are described by tool owners, and explain how the tools can help to manage the threats. The set of threats covered in this deliverable also serves as an example to help use case owners describe the threats they are typically confronted with.

In its initial version, the security knowledge base contains generic security threats, including but not limited to remote exploits, such as denial of service attacks, remote injections or snooping attacks software bugs, causing a host to become unreliable or unavailable unauthorised local access, where an attacker gains physical access to hardware, enabling them to steal data or alter processes or hardware Furthermore, secondary threats are covered, i.e. threats that appear when a precondition exists. These secondary effects cause other assets to misbehave. This means that they can be chained into “secondary effect chains”, where a set of root causes can cause a whole tree of secondary effects and misbehaviours in related assets.

3.3 Validation of WP5

This work package is divided in three parts:

- *Consent Management*: aims to provide support for initial evaluation of the architecture and functionality. SHiELD will provide an integrated system to manage and enforce patient consent preferences. A decision engine and administration point will allow authorization policies to be defined

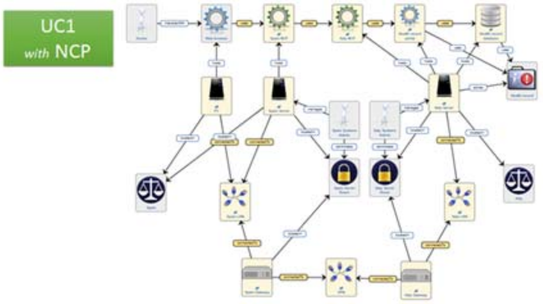
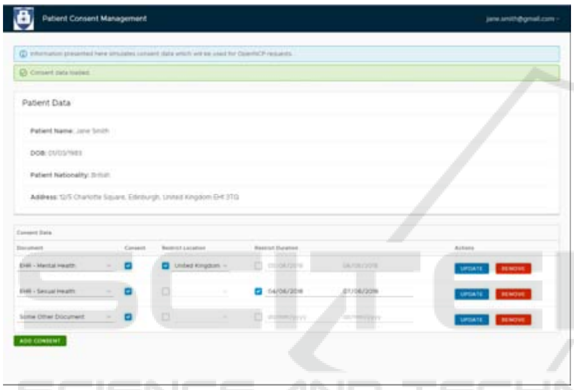


Figure 6: Use Case 1 represented in System Modeller tool.

and evaluated giving greater flexibility than traditional authorization approaches. All this will be done through consent UI and database will facilitate the input and storage of patient consents at a fine-grained level.



Information presented here simulates consent data which will be used for OpenNCP requests.

Consent data loaded.

Patient Data

Patient Name: Jane Smith

DOB: 01/03/1983

Patient Nationality: British

Address: 12/5 Charlotte Square, Edinburgh, United Kingdom EH 3TG

Consent Data

Document	Consent	Restrict Location	Restrict Duration		Actions
EHR - Mental Health	☑	☑ United Kingdom	□ 01/06/2018	08/06/2018	UPDATE REMOVE
EHR - Sexual Health	☑	□	☑ 04/06/2018	07/06/2018	UPDATE REMOVE
Some Other Document	☑	□	□ dd/mm/yyyy	dd/mm/yyyy	UPDATE REMOVE

ADD CONSENT

Figure 7: Consent Management User Interface.

- *Sensitivity Tool and Data Hiding Tool*: The process of identifying sensitive data is a necessary step to be able to address EU GDPR regulation which aims primarily to give control to EU citizens and residents over their personal data. The first step to address the GDPR regulation is to find the sensitive/personal data in the organization data stores. Once the sensitive data has been identified, the organizations can provide their customers/users the ability to control (delete, modify etc.) their personal data.

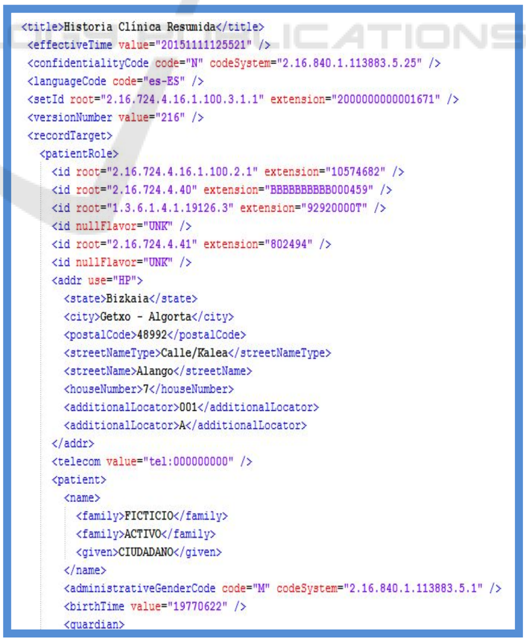
The Data Sensitivity Analysis Tool addresses this step. It finds the sensitive/personal data in relational databases. For each column in the database, the tool indicates if the column is sensitive or not and provides a confidence score (a value between 0.0 and 1.0). The confidences core indicates how much the tool is confident that the specific column is indeed sensitive. In addition, the tool provides explanations why a specific column is considered as sensitive. This is done by displaying additional categories the column belongs too.

The tool itself is configurable. The tool contains a library of data classifiers, each finds if a column belongs to a specific category. In addition, it enables adding additional categories by adding corresponding data classifiers.

The users configure the sensitive classification problem by selecting which categories are related to the problem, and how they relate to the sensitivity category. For example, a user may decide that a column is sensitive if it is either email, or social-id. In addition, the user declares a threshold. A column belongs to a specific category only if its confidence score is above the threshold. Then, data masking is the process by which sensitive data is replaced, possibly in a reversible manner, with data that is unintelligible to receiver. The masked data is usually sensitive data, such as personally identifiable information, health information, names, addresses, and so on.

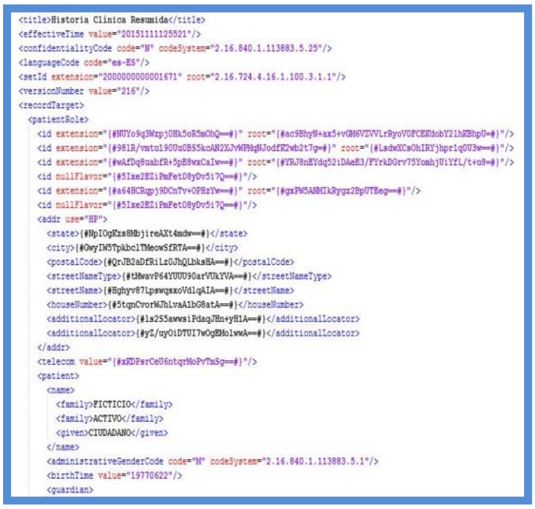
The main purpose of data masking is to preserve the data owner privacy enforce the data owners consent and comply with legal regulation (such as GDPR).So these figures that appear below (number 8 and 9), show how the fields of the Patient Summary from the Spanish side are masked.

There is an output of the masking tool showing how patient details -state, city, postal code, street etc. - in the data (sample) can be masked (encrypted) as well as unmasked (decrypted).



```
<title>Historia Clínica Resumida</title>
 <effectiveTime value="20151111125521" />
 <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25" />
 <languageCode code="es-ES" />
 <setId root="2.16.724.4.16.1.100.3.1.1" extension="2000000000001671" />
 <versionNumber value="216" />
 <recordTarget>
   <patientRole>
     <id root="2.16.724.4.16.1.100.2.1" extension="10574682" />
     <id root="2.16.724.4.40" extension="BBBBBBBBBB000459" />
     <id root="1.3.6.1.4.1.19126.3" extension="92920000T" />
     <id nullFlavor="UNK" />
     <id root="2.16.724.4.41" extension="802494" />
     <id nullFlavor="UNK" />
     <addr use="HP">
       <state>Bizkaia</state>
       <city>Getxo - Algorta</city>
       <postalCode>48992</postalCode>
       <streetNameType>Calle/Kalea</streetNameType>
       <streetName>Alango</streetName>
       <houseNumber>7</houseNumber>
       <additionalLocator>001</additionalLocator>
       <additionalLocator>A</additionalLocator>
     </addr>
     <telecom value="tel:000000000" />
     <patient>
       <name>
         <family>FICTICIO</family>
         <family>ACTIVO</family>
         <given>CIUDADANO</given>
       </name>
       <administrativeGenderCode code="M" codeSystem="2.16.840.1.113883.5.1" />
       <birthTime value="19770622" />
       <guardian>
```

Figure 8: Spanish Patient Summary no masked.



```
<title>Historia Clínica Resumida</title>
<effectiveTime value="20151111125521"/>
<confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
<languageCode code="es-ES"/>
<setId extension="2000000000001671" root="2.16.724.4.16.1.100.3.1.1"/>
<versionNumber value="216"/>
<recordTarget>
  <patientRole>
    <id extension="{#NUYo9q3Wzpj0Hk5oR5m0hQ==#}" root="{#ac9BhyN+ax5+vGM6VZVVLrRyoV0FCEKdobY21hKBhpU=#}"/>
    <id extension="{#981R/vmtu190Uu0BS5kcAN2XJvWPMqNJodfK2wb2t7g=#}" root="{#LsdwXCs0hIRYjhpr1q0U3w==#}"/>
    <id extension="{#wAfDq8uabfR+5pE8wxCaIw==#}" root="{#YRJ8nEYdq52iDAeE3/FYrkDGrv75YomhjUiYfL/t+u8=#}"/>
    <id nullFlavor="{#5Ixe2EZiPmFet08yDv5i7Q==#}"/>
    <id extension="{#a64HCRqpj9DCnTv+OPHzYw==#}" root="{#gxPW5ANMIkRygz2BpUTEeg==#}"/>
    <id nullFlavor="{#5Ixe2EZiPmFet08yDv5i7Q==#}"/>
    <addr use="HP">
      <state>{#NpIOgKzs8MbjireAXt4mdw==#}</state>
      <city>{#GwyIW5TpkbclTMeowSfRTA==#}</city>
      <postalCode>{#QrJB2aDfRiLz0JhQLbksHA==#}</postalCode>
      <streetNameType>{#tMwavP64YUUU9OarVUkYVA==#}</streetNameType>
      <streetName>{#Hghyv87LpswqsxoVdlqAIA==#}</streetName>
      <houseNumber>{#5tqnCvorWJhLvaA1bG8atA==#}</houseNumber>
      <additionalLocator>{#ls2S5awwsiPdaqJHn+yH1A==#}</additionalLocator>
      <additionalLocator>{#yZ/uyOiDTUI7wOgEMolwwA==#}</additionalLocator>
    </addr>
    <telecom value="{#xKDPsrCeU6ntqrMoPvTmSg==#}"/>
    <patient>
      <name>
        <family>FICTICIO</family>
        <family>ACTIVO</family>
        <given>CIUDADANO</given>
      </name>
      <administrativeGenderCode code="M" codeSystem="2.16.840.1.113883.5.1"/>
      <birthTime value="19770622"/>
      <guardian>
```

Figure 9: Spanish Patient Summary masked.

- *Mobile Devices Security Prototype*: In its current state, the prototype uses hardware features to demonstrate the ability to detect device tampering. Moving forward, additional feature types will be integrated to determine who is operating a device, and in what context. The hardware features that will be utilized are evolving, with the feature mappings still being refined and improved upon. Further methods of delivery are also continuously being evaluated.

3.4 Validation of WP6

During the execution of WP6, a user interface has been developed to simulate real-time access to patient data, which is exchanged through the OpenNCP nodes. The user interface has three different roles for accessing to different level of clinical data (Figure 10):

- administrative staff; only has access to administrative data;
- nurse: only has access to patient summary;
- doctor: has access to all clinical data that the patient has consent to be exchange.

From a Spanish hospital, to access the application, the administrative staff must enter their own credentials to access the system. This obviously will be required for each healthcare professional involved in the system (i.e., administrative staff, nurse, medical doctor).

Once the professional is logged into the application, he has to fill the patient's personal data in the system for searching it in the Italian Health System.

Then, the italian OpenNCP request info to the Spanish OpenNCP and returns a list of patients from Italian Health System.

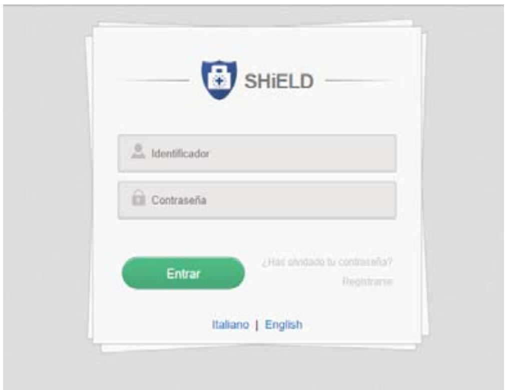


Figure 10: Access system screen.

The professional has to click in the button *"Watch patient"* for seeing the clinical data related to the patient from the Spanish System. Once the patient is chosen, his/her personal information appears in the SHiELD Application.

Apart from seeing the personal data, the administrative has to click in the button *"Generate episode"* for registering the patient in the Italian system and then, the nurse is who do the triage (the triage process, after some basic tests like taking the temperature, blood pressure check and so on, the patient gravity is rated to locate them in the system with the proper priority).

The nurse would be able to check also the patient's Medical Prescriptions and Personal History.

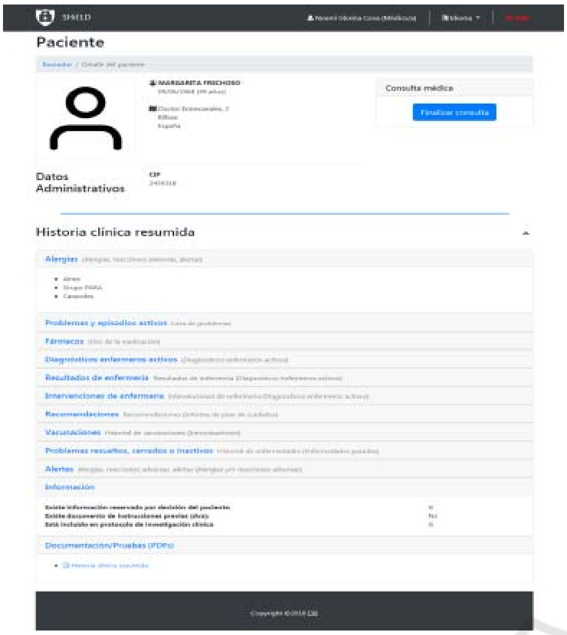
After this, the doctor can see which patient is pending for consultation, order by the gravity.

The doctor can see the all clinical records not only on the screen but also in PDF document.

4 CONCLUSIONS

Security challenges need to be addressed by the SHIELD project for the eHealth domain. Among others, the challenges are: interoperability, confidentiality, availability, integrity, privacy, regulations and eHealth data. Which data are going to be shared and by which mean? The first validations will be useful as the basis for both the "in depth" requirements analysis for the platform as well as setting the main pillars for the SHIELD architecture detailed design.

SHiELD will unlock the value of health data to European citizens and businesses by overcoming security and regulatory challenges that today prevent



SHIELD [illegible] (Médico/a) Idioma

Paciente

Buscador / Detalle del paciente

MARGARITA FRECHOSO
[illegible]

Doctor Entrecanales, 2
Bilbao
España

Consulta médica

Finalizar consulta

Datos Administrativos

CIP
[illegible]

Historia clínica resumida

Alergias (Alergias, reacciones adversas, alertas)

- [illegible]
- Grupo PARA
- [illegible]

Problemas y episodios activos Lista de problemas

Fármacos (Uso de la medicación)

Diagnósticos enfermeros activos (Diagnósticos enfermeros activos)

Resultados de enfermería Resultados de enfermería (Diagnósticos enfermeros activos)

Intervenciones de enfermería Intervenciones de enfermería (Diagnósticos enfermeros activos)

Recomendaciones Recomendaciones (Informe de plan de cuidados)

Vacunaciones Historial de vacunaciones (Inmunizaciones)

Problemas resueltos, cerrados o inactivos Historial de enfermedades (Enfermedades pasadas)

Alertas Alergias, reacciones adversas, alertas (Alergias y/o reacciones adversas)

Información

Existe información reservada por decisión del paciente: Si
Existe documento de instrucciones previas (dvs): No
Está incluido en protocolo de investigación clínica: Si

Documentación/Pruebas (PDFs)

- Historia clínica resumida

Copyright ©2018 [illegible]

Figure 11: Doctors' view.

this data being exchanged with those who need it. This will make it possible to provide better health care to mobile citizens across European borders, and facilitate legitimate commercial uses of health data.

REFERENCES

Boone, KW. The CDA TM book. Springer-Verlag London: 2012.

eHealth DSI Semantic Community. Clinical Documents: CDA Implementation Guides. https://ec.europa.eu/cefdigital/wiki/display/EHSEMANTIC/Clinical+Documents%3A+CDA+Implementation+Guides (accessed on October 2018).

epSOS D3.2.2 Final definition of functional service requirements- Patient Summary and Glossary of terms.https://openncp.atlassian.net/wiki/spaces/ncp/overview?mode=global (accessed on October 2018).

European Commission. 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 (OJ l 88, 4.4.2011, p.45), 2011.

European Commission. eHealth action plan 2012–2020. http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf (accessed on October 2018).

European Commission. GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the EU. 2016 L 119, page 1.

Health Level Seven International - HL7 Implementation Guide for CDA® Release 2: IHE Health Story Consolidation, DSTU Release 1.1 (US Realm), Draft Standard for Trial Use, July 2012. https://www.hl7.org/implement/standards/product_brief. cfm?product_id=258 (accessed on October 2018).

Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: A systematic review. Technol Health Care. 2016; 24(1):1-9.

Minor LB. Report Harnessing the Power of Data in Health. Stanford University School of Medicine 2017. https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf (accessed on October 2018).

Pocs M. Will the European Commission be able to standardize legal technology design without a legal method? Comput Law Secur Rev. 2012; 28: 641-650.