11th EUROPEAN CONGRESS ON EMERGENCY MEDICINE
MEGARON ATHENS INTERNATIONAL CONFERENCE CENTER
23-27 September 2017 Athens EUSEM2017

European security in health data exchange. A challenge at emergency departments.

Eunate Arana-Arri[1], Aitor García de Vicuña[1], Miguel Angel Ogueta[2], Santiago Rodríguez[1], Oscar Perez[1], Ines Gallego[1] and Maria Luz del Valle[1]
[1]BioCruces Health Research Institute-Cruces University Hospital - Barakaldo – SPAIN
[2]HAssistive Quality.Osakidetza - Vitoria-Gasteiz – SPAIN

Background:

Security is one of the main challenges when applied to eHealth and is crucial in the transmission of required data around patients and citizens when travelling around the world. This is the aim of European funded SHiELD project. One of the specific developments to be done in SHiELD is the end-to-end systemic analysis of potential risks to health data. This will be achieved by creating a knowledge base from potential threats including 'classical' cyber security threats, emerging threats to personal data, and compliance threats.

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

Patients & Methods :

SHiELD will unlock the value of health data to European citizens and businesses by overcoming security and regulatory challenges that today prevent this data being exchanged with those who need it, especially in emergency situations when access to key data needs to be achieved in a short period of time. One of the European projects dealing with the security and interoperability of eHealth data is epSOS project's that result is the OpenNCP architecture and implementation. The OpenNCP community has designed and developed a set of Open Source Components based on the services developed in epSOS that can be used by Participating Nations to build their local implementation of an NCP. However, this has not been validated and put into practice.

Results & discussion :

Validation scenarios (realistic use cases), will be supported by three different member states (Italy, United Kingdom and Spain). In all scenarios, we assume a citizen travels abroad and they need or demand health care; the foreign healthcare professional needs to access and/or manage patient's health records. One of the scenarios that will be validated is an Italian citizen travelling to Spain that has acute emergency (e.g. stroke) and loses consciousness. Spanish emergency department suddenly assists the patient. After the first aid, the emergency doctor wishes to check the patient's health record to know his/her medical history (e.g. epSOS patient summary). Will those data suffice? Which are the mandatory minimum data and how systems will secure them? SHiELD will also build upon examples: last known activities (e.g. mobile/wearables with heart rate, blood pressure,...) from "Get Active" in the United Kingdom

Figure 1: Data exchange scenario

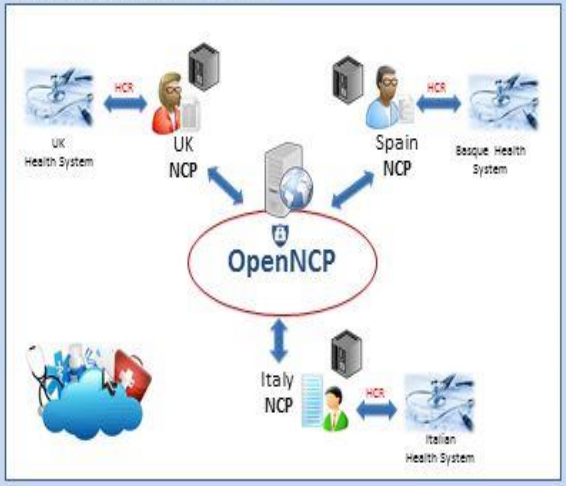


Figure 2: Final trial scenario

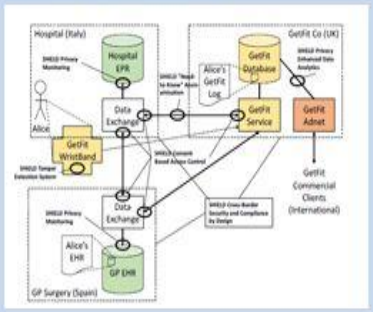
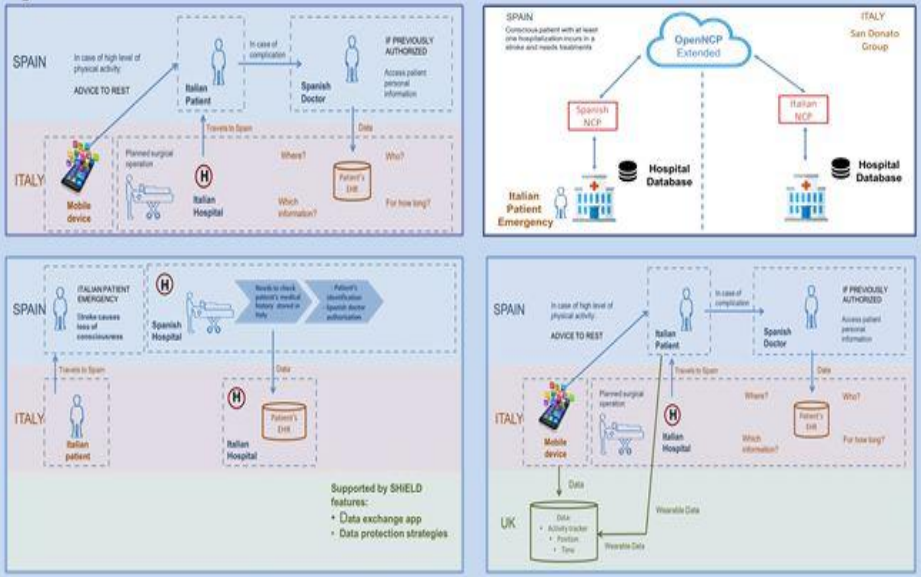


Figure 3: Patient clinical data

Figure 4: Use cases for the validation



Conclusion & perspectives :

Security challenges need to be addressed by the SHiELD project for the eHealth domain. As summary these challenges are: interoperability, confidentiality, availability, integrity, privacy, regulations and eHealth data (identify which data are going to be shared and by which mean). This will be used as the base for both the "in depth" requirements analysis for SHiELD as well as setting the main pillars for the SHIELD architecture detailed design.

Grant: H2020-DS-2016-2017 (Digital Security Focus Area)
Type of action: RIA (Research and Innovation action)