NGI THINK NEXUS

Policy Brief 2

Blockchain and Big Data analytics for eHealth:

A topic for collaboration between EU and US

Policy Brief writen by:
Think NEXUS Science & Technology
Expert Group

Think NEXUS, an EC-funded project, aims at reinforcing EU-US collaboration on NGI-related topics in three focus areas: Science and Technology, Innovation and Entrepreneurship and Policy. The aim is to boost strategic research, industrial partnerships and policy compliances in order to gain socio-economic benefits in both the EU and US regions.

In the framework of this project, we are regularly publishing several short articles aiming at comparing the US and the EU approaches in different topics of NGI. The present document is focusing on Artificial Intelligence.

THI

NK

NEX

US

Blockchain and Big Data analytics for eHealth: A topic for collaboration between EU and US

Vast amounts of health data are now produced, gathered and stored in electronic health records (EHRs) in multiple formats, during citizens' medical examinations both across Europe and the US. This is largely a result of the explosion of available technological devices and medical services, which are nowadays used by citizens. Citizens and health-oriented entities generate data but the data do not flow among these entities in a seamless, cohesive and standardized way. Rather, healthcare involves a diverse set of public and private data collection isolated systems ("silos"), including health surveys, administrative enrolment, billing records, and medical records, used by various entities such as hospitals, medical doctors, health authorities, pharmacies or even citizens in different countries and regions.

Currently there is no easy and standard way or capability to gather data about citizens from these silos. The fragmented landscape is a serious set-back against deploying integrated applications that could provide better and more accurate diagnosis, aid faster research outcomes and more. The prospects of integrated health data raise the need for better integration and sharing of data within and across healthcare systems, organisations and countries.

However, most of the healthcare services and entities operate independently and use heterogeneous systems for managing health data, which makes it difficult to obtain and integrate information from different sources in the healthcare domain. Thus, opportunities to reuse this data for research and better healthcare are often missed due to the lack of data interoperability and complexity of dealing with different systems or data silos, as well as lack of standardized processes for data anonymization which would allow data sharing with respect to users' privacy.

In addition to the technical challenges of integrating health data, the sensitive nature of the data raises many security and privacy concerns about its processing, storage and utilisation. Recent security (e.g. NHS ransomware attack in 2017[1] and privacy (e.g. exploitation of personal information by Cambridge Analytica in 2018[2]) scares have raised the general awareness about the protection and privacy of data. Moreover, a broad range of new healthcare technologies

1 NHS cyber-attack: Everything you need to know about 'biggest ransomware' offensive in history, Available at: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

2 Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, Available at: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

(e.g. mobile applications and wearables) threaten to break apart the protections of existing regulations and expose the long-existing gaps in individual rights.

Therefore, any approach for data integration and management would need to be open and transparent in terms of the security and privacy mechanisms that are being put in place in order for citizens to willingly entrust the approach. Likewise, it should be compliant to the emerging GDPR (established in the EU, but already having global impact), which remedies several security, privacy and data protection concerns. However, healthcare companies are notorious for their limited investments in security, as highlighted in the 2016 HIMSS Analytics Healthcare IT Security and Risk Management Study.

For example, the US federal government spends 16% of its IT budget on security[3] , while ABI Research estimates that investments in the industry against cyber-attacks will only reach $10 billion worldwide by 2020[4] . Another issue currently faced by healthcare organizations is that they have sensitive data spread across a number of devices, not just servers and desktops but also laptops, mobile devices, and specialized devices for inputting medical record data. According to Healthcare Breach Report[5] , 68% of all healthcare data breaches since 2010 were due to device theft or loss, which basically addresses the citizen-generated data.

To unlock the full potential of eHealth innovation and recent extremely fast developments, while curtailing potential negative consequences and practices, effort must be invested in standardisation and harmonization, data privacy and security. These efforts should enable citizen empowerment, since healthcare reliance has changed from an isolated system to a critical infrastructure. Interoperability and security measures must support the secure data exchange and utilisation across the interconnected health system, while facilitating citizens contributions (through ethical sourcing of the user generated social and quantified-self data) and ensuring transparency.

Collaboration between EU and US stakeholders is critical. Focus should be given in co-developing technologies and applications that will allow an interoperable exchange of health information across regions based **on a citizen-centric approach that provides citizens (and other data providers) with full control over their personal data**. In this direction, research activities should be focusing on **blockchain as a key underlying infrastructure** ensuring that data contribution, sharing, exchange, use and processing will follow **citizens consent** and needs to be **fully secure and optimized for different stakeholders in the healthcare ecosystem that will be authorized to access them: citizens, hospitals, medical doctors, health professionals and pharmacies.**

3 Federal Spending: Where Does the Money Go, Available at: https://www.nationalpriorities.org/budget-basics/federal-budget-101/spending/

4 Risks to Drive US$10 Billion Cyber Insurance Market by 2020, Available at: https://www.abiresearch.com/press/risks-to-drive-us10-billion-cyber-insurance-market/

5 Bitglass Report: Breached Healthcare Records Hit Four-Year Low, Available at: https://www.bitglass.com/press-releases/healthcare-breach-report-2018

NGI THINK NEXUS

thinknexus.ngi.eu @ThinkNEXUS_NGI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825189. This publication reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains