# EPI infrastructure: A dynamic infrastructure to secure data sharing in healthcare applications

Jamila Alsayed Kassem[1]

[1]UvA, MNS group

The EPI (Enabling Personalised Interventions) [1]project aims to provide self/joint management of medical treatments throughout the healthcare cycle by effectively utilising data usage with scientific algorithms. And as an end result, the EPI project processes health data having various sources, governance, and ownership to formulate a personalized outcome of diagnostics, prevention, advice in a real-time effective manner, hence acting as a health digital twin. A data sharing infrastructure is needed in order to efficiently and securely share health data to make EPI possible. And the research question to be answered is, *how to build a single ICT infrastructure architecture to enforce different set of requirements and secure health data sharing supporting different use cases?*

According to previous surveys [4], roughly 15% of patients visiting a doctor were asked to supply their radiology report personally (like on a DVD), and another 5% had to redo their tests. Even though physical sharing can be secure (not available on a public network), the copy can be easily lost/misplaced/stolen. Moreover, this is not optimal in practice. Traditional ways don't work for big data sharing, hence hinder research and other applications (digital health twin, live streaming, etc.). Subsequently, due to the impractical data sharing methods, its limitations. and combined with the latest advancements in the field of informatics, a lot of research applicable in the health domain was inspired.

There is a wide consensus that sharing data in the medical spectrum can be beneficial in terms of cost efficiency, preventing redundancies, cooperation between stakeholders, reliable research by accelerating innovations and discoveries. Achieving secure health data sharing can result with an efficient and effective health care cycle managed by the patients/Health care stakeholders. Researchers proposed different framework with that goal in mind. Recent papers introduced sharing data via blockchain [3][6][1] that leverage an established consensus on a blockchain ledger over third party intermediates. Other papers used emerging tools like 5G, IoT networks, edge computing to monitor and stream big chunk of health data [5][2].

To the the best of our knowledge, the idea of a dynamic health data sharing infrastructure is not yet covered by literature. A dynamic health infrastructure is the concept of changing the infrastructure to enforce a different set of rules for a specific duration of time with the aim of supporting numerous use cases. The majority of the proposed work seems to be application specific, and all shared resources are exclusively data (no algorithm or intermediate results). These infrastructures are mainly static and still offer a "one fits all" security standards. There are different security requirements to be considered depending on the application request, end point of data sharing, type of data. etc. With that into account, no one ICT infrastructure is developed to support different uses cases inputting different requirements.

Our research goal and the focus of the ICT.Open poster presentation is to enforce tailored security requirements/ application scenario. The architecture has several requirements which are addressed as illustrated in fig 1.

The three main requirements that are considered are *dynamicity, rule enforcement, and fault control*. Firstly, the architecture supports different use case by re-initialising the infrastructure / application request. The application translates to a set of rules to dictate the allowed information flow from network nodes n and n' (top fig 1). Also, there's another set of security attributes that can be offered/ network

[1]https://delaat.net/epi/

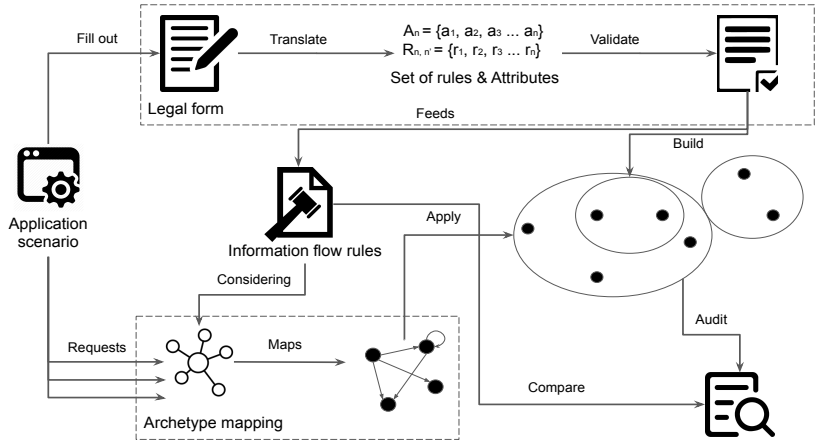


Figure 1: The EPI architecture

node n. That is further verified and used to feed the information flow rules log and segregating nodes into security areas in the infrastructure of relevant nodes to the scenario. Secondly, enforcing rules is made easier defining security area to each node and introducing a gatekeeper. Lastly, fault control ensures accountability via auditing (bottom left fig 1).

As a result, we will be able to tailor the architecture abiding by rules influenced by the application scenario hence having a dynamic infrastructure. In the future, we expect to apply a specific use case, then test and evaluate the method used. The limitations that we foresee encountering are mainly: verifying rules according to laws and international policies, acceptability of the framework by health institutions, and the integration of it. We address that by working closely with legal experts and along side hospitals and ethical boards.

# References


[1] FAN, K., WANG, S., REN, Y., LI, H., AND YANG, Y. Medblock: Efficient and secure medical data sharing via blockchain. *Journal of Medical Systems 42*, 8 (Jun 2018), 136.

[2] MANOGARAN, G., VARATHARAJAN, R., LOPEZ, D., KUMAR, P. M., SUNDARASEKAR, R., AND THOTA, C. A new architecture of internet of things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generation Computer Systems 82* (2018), 375 – 387.

[3] PATEL, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal 25*, 4 (2019), 1398–1411. PMID: 29692204.

[4] PATEL, V., BARKER, W., AND SIMINERIO, E. Trends in consumer access and use of electronic health information. *Office of the National Coordinator for Health Information Technology: Washington DC.* (October 2015).

[5] THILAKANATHAN, D., CHEN, S., NEPAL, S., CALVO, R., AND ALEM, L. A platform for secure monitoring and sharing of generic health data in the cloud. *Future Generation Computer Systems 35* (2014), 102 – 113. Special Section: Integration of Cloud Computing and Body Sensor Networks; Guest Editors: Giancarlo Fortino and Mukaddim Pathan.

[6] XIA, Q., SIFAH, E. B., ASAMOAH, K. O., GAO, J., DU, X., AND GUIZANI, M. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access 5* (2017), 14757–14767.