

# Health Data Sharing Across Jurisdictions: Business and Legal Perspectives: *Use Case Analysis*

Koel Ghorai<sup>\*</sup>  
Jan M. Smits<sup>\*\*</sup>  
Maarten Kluitman<sup>\*\*\*</sup>  
Pradeep K. Ray<sup>\*</sup>

**Abstract:** *Online health data sharing and transfer has become easier and more efficient than ever before in recent times. However, this has also led to data oriented challenges around privacy and protection. While transfer of sensitive health as well as personal data between organizations and countries requires high level of protection and privacy, most people involved in business processes in the service industry, especially one as complex as healthcare, are generally oblivious of the legal responsibilities and implications of data privacy regulations. In this paper, we propose a new framework that combines business and legal aspects of any health related business process in relation to protection and privacy of sensitive data exchange. This framework encompasses patients, businesses and organizations and includes an approach for considering legal regulations as well as factors that may affect privacy and security of data such as health data in business processes. Using the proposed framework, we have further analyzed an online healthcare patient registration process for an aged care provider as part of a European Union project involving several European countries and Australia. It also considers the applicability to the various process components within the context of European privacy laws.*

**Keywords:** *data privacy, security, business framework, legal framework, privacy regulation.*

## I. Introduction

Technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the country and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data. In spite of various privacy and security frameworks that exist for health data protection [1], a need for a business and legal framework has been identified [2] that can be used for analyzing business as well as regulatory aspects when it comes to sensitive health data

---

<sup>\*</sup> University of New South Wales

<sup>\*\*</sup> University of Technology Eindhoven

<sup>\*\*\*</sup> Independent

<sup>\*</sup> University of New South Wales

exchange across organizations. In this paper, we have proposed a unique framework that combines business process and legal components for analyzing the privacy and security aspects of sensitive data exchange. Our framework resorts to the mapping of business process components and data to legal regulations. This paper also focuses on the analysis of an online patient registration process for a non for profit organization using the proposed framework. This is part of an ongoing research AU2EU for the European Union's 7th Framework Programme (FP7).

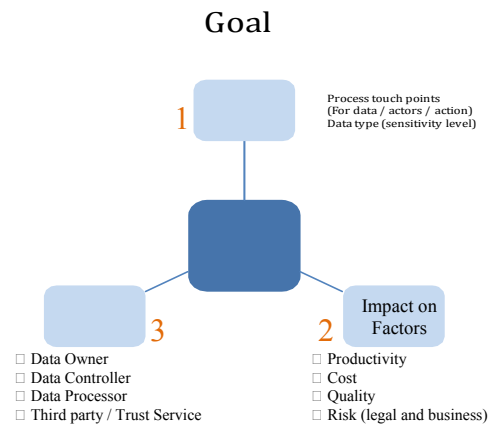
## **II. Background**

Various business models and legal frameworks exist for analysis of business processes [3]. Darimont et al [4] provide a goal oriented approach for analysis of regulations by transforming regulation documents in to three models for goals, objects and threats. But it does not combine all the three models together. An integrated model would help in improved traceability in a process. Rifaut et al [5] present a goal based model for implementation of financial system complying with the Basel II regulations. The model defines the objectives, strategies and policies for each organizational layer and model for designing a regulation compliant financial system. This model also does not help the users to identify the individual or organization liable in case of non-compliance of data regulations. None of the models present a combined framework for identifying the privacy regulations and align them to the business processes. The framework introduced in this paper demonstrates how the data privacy regulations can be aligned to business processes dealing with highly sensitive health data. The framework incorporates various stages including identification of business process components, data types and assurance levels in addition to identification and application of appropriate regulations for data privacy and security.

## **III. Combined Business and Legal Framework**

### *A. Identifying Business Process Components*

A business process is a set of logically related business activities that combine to deliver something of value (e.g. products, goods, services or information) to a patient [6]. A business process can be seen as a set of activities that create a value chain for an organization and associate the value chain with the requirements of the subjects involved in the process. Thus, it is important to identify the various components of the process to be able to successfully understand and analyze the value chain and map it to the required level of security and privacy. To achieve this goal, a general business process model with its various components has been developed.



*Fig. 1. Business process model and its components*

The model consists of three main components:

### **Actors**

An actor is a person or an organization or a legal entity that can participate in an activity. Four types of actors have been identified in the business process model.

- **Data Subject:** A data subject is a natural person that can be identified, directly or indirectly, in particular by reference to an identifier; such as a name, an identification number, location data, to an unique identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, social, or gender identity of that person.
- **Data Controller:** A data controller is a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
- **Data Processor:** 'Processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction. According to applicable laws, a data processor can be a legal person, a public authority, an agency or an electronic platform that carries out the operation or set of operations detailed under "processing".
- **Third Party:** Is any natural or legal person, public authority, agency, or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

## Activity

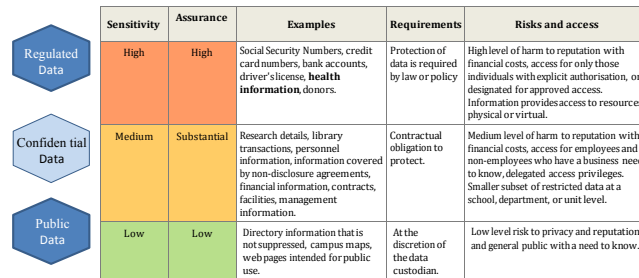
An activity can be described as an action undertaken by the involved actors for the purpose of generating profits or developing economic opportunities. An activity has three main components. These are:

- Goals: are the objectives for undertaking an activity.
- Touch point: describes all activities with involvement of the components (actors and their actions).
- Resource (Data): Resource is a component of the business process that can be shared physically or electronically between the actors. Resource applies to any kind of data, most importantly, "personal data", which can be defined as any information relating to an identified or identifiable natural person ('data subject').

Since the impact of the activities on a business process factors is not within the purview of this paper, it has not been described in details.

### B. Data Types and Assurance Levels

A business process involves exchange of data which can be personal, organizational, national as well as international. Whenever transaction of data is concerned, there are legal issues which are involved in the process. In order to map the data transactions to legal aspects, data has been categorized into three types according to the level of sensitivity, as given in figure 2 below. This will pave the way for mapping data to the legal framework.



	Sensitivity	Assurance	Examples	Requirements	Risks and access
Regulated Data	High	High	Social Security Numbers, credit card numbers, bank accounts, driver's license, <b>health information</b> , donors.	Protection of data is required by law or policy	High level of harm to reputation with financial costs, access for only those individuals with explicit authorisation, or designated for approved access. Information provides access to resources, physical or virtual.
Confidential Data	Medium	Substantial	Research details, library transactions, personnel information, information covered by non-disclosure agreements, financial information, contracts, facilities, management information.	Contractual obligation to protect.	Medium level of harm to reputation with financial costs, access for employees and non-employees who have a business need to know, delegated access privileges. Smaller subset of restricted data at a school, department, or unit level.
Public Data	Low	Low	Directory information that is not suppressed, campus maps, web pages intended for public use.	At the discretion of the data custodian.	Low level risk to privacy and reputation and general public with a need to know.

Fig. 2. Types of data and Level of Sensitivity

## IV. Combined Business & Legal Framework

The legal aspects in combination with the Business Process Model (as given in Figure 1), can be used for analyzing various use cases in different scenarios. Analysis of a use case has been carried out using the following steps.

A. Identifying Actors and Activities

- Identify Actor: Actors of each use case have been identified as a "Data subject", "Data Controller", "Data Processor" or "Third Party",
- Identify Resource: The resource, in this context, is data. It can be public, confidential or regulated data with varying levels of sensitivity associated with it (refer to figure 2 for details),
- Identify Action: In this context, the activity involves "data sharing" and all processes associated with it.

B. Validation of Data Sensitivity

Following the activity description, the level of sensitivity of the transferred data is validated, based on the content of the data. The data, which is exchanged between actors in the business process, is classified as having three levels of sensitivity, as portrayed in figure 2, the three levels of sensitivity are low, medium and high.

C. Identification of appropriate regulations for e- Authentication and e-Authorisation

The third step involves the identification and application of appropriate legislations and regulations. These regulations and legislations are specific to each country or union

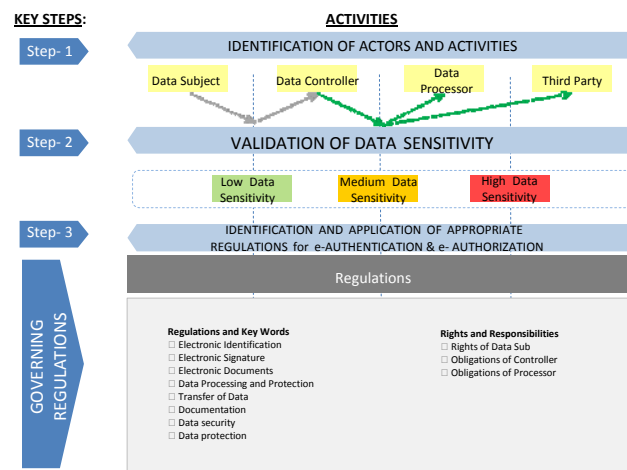


Fig. 3. Combined Business and legal (CBL) framework

V. Application of Combined Framework to Online Patient Registration (use case)

Increasing use of electronically authenticated and authorized electronic platforms for replacing paper based processes are of strategic importance for achieving efficient and sustainable growth objectives for organizations, especially in the healthcare sector. This increases the need for proper legal regulations and laws in places for online data privacy

and exchange. This case study describes the use of electronic authentication and electronic authorization for online patient registration process at an Ambient Assisted Living service provider. The electronic platform significantly improves the security and safety of highly sensitive patient data by introducing means for electronic authentication and electronic authorization. It also saves cost and time by improving efficiency of the service providers' employees in addition to improving quality and integrity of patient data upload, as well as efficiency and convenience in data accessibility for registration process. The combined business and legal framework has been aligned to the online patient registration process as an example of the framework application in a real life scenario.

#### *A. Healthcare Service Provider's Online Patient Registration Process*

In the service provider's online patient registration process, an e-Authentication and e-Authorization platform is adopted which enables the organization to confidentially store and transfer patient data. Figure 4 depicts the online patient registration process in the case of the Ambient Assisted Living (AAL) service provider. By adopting the e-Authentication/e- Authorization platform, a field representative of the service provider registers patient data remotely on a mobile device (e.g. a tablet), and transfers the patient data automatically to the Home Emergency Call (HEC) server located at the service provider's premises.

When the patient requests a registration, the service provider dispatches a field representative, who gathers the patient's personal data including health information which is highly sensitive and requires to be secured and protected through proper means of authentication and authorization. Therefore, a secure connection between the mobile device and the e-Authentication/e-Authorization platform server is established, and the field representative has to authenticate with the server. In addition, the terminal the representative uses for entering patient data has to be secure and its trustworthy status has to be verifiable at any time. Having a secure terminal together with encrypted channels to the e-Authentication/e- Authorization platform servers and finally a privacy-aware computation of the data on the server, builds a chain of trust to guarantee each patient that sensitive personal data is handled in good faith and with due diligence. Through this secured connection, the patient data can directly be entered into the service provider's patient database by the field representative. Then, the server generates the contract details (accounting information, pricing, insurance coverage, etc.) and transfers it to the mobile device of the field representative. To conclude the mobile device presents a signature field which finalizes the registration process.

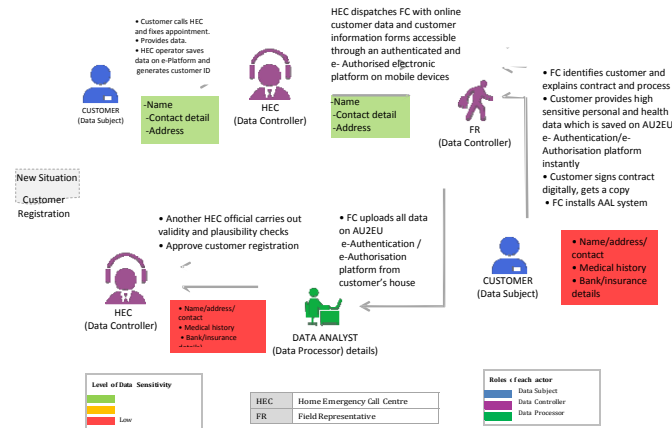


Fig. 4. Online Patient Registration Process

A digital copy of the contract is mailed to the email address of the patient or a paper based copy is provided in case the patient doesn't have access to internet connection or an email address. The field representative then directly installs and configures the AAL system at the patient's home. A possible addition to the e-Authentication/e-Authorization platform services is the option to retrieve personal data from external data sources (e.g. hospitals for medical records and the municipality for housing and general contact details, or from the AAL system analysis server, to check the activity of AAL sensor devices).

In figure 4, the data that is exchanged at various stages is color coded as green, red and yellow depending on the level of sensitivity (refer to figure 2 for details). The data sensitivity categorization is done based on the kind of data which is exchange

*B. Mapping CBL Framework to Patient Registration Use Case*

The online patient registration process has been mapped to the Combined Business and Legal (CBL) framework (as mentioned in figure 3). The CBL framework, including this mapping, is given in Figure 5. Mapping the CBL framework to the AAL registration process provides an overview of the activities, actors, action and the legal rights and regulations binding the various actors. In this case, the main activities involve data sharing. The data that is shared has been categorized according to its level of sensitivity and the levels of e-Authentication and e-Authorization procedures are proportional to the level of data sensitivity. The higher the sensitivity, the higher is the risk involved and this will lead to implementation of stricter e-Authentication and e-Authorization procedures. The regulations pertaining to electronic transactions [7] have been selected for this use case. These include rights and obligations of the actors involved. The legislations have been mentioned as articles in Figure 5.

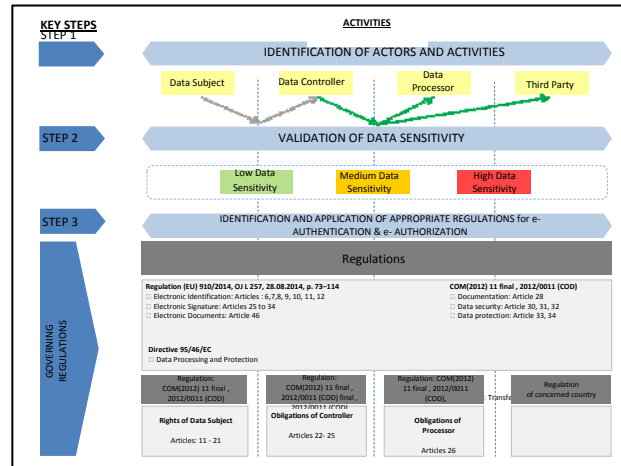


Fig. 5. Mapping Patient Registration process to CBL Framework

### Identification of Actors

The actors of the online AAL patient registration use case have been categorized into four distinct groups. The patient is the data subject. The healthcare service provider is the data controller. The field representative is an employee of the service provider, hence he is considered as the data controller. The database services are rented by the service provider and these database service providers have been categorized as data processors. Thus the database as well as the e-Authentication/e- Authorization platform, in this case, has been considered as the data processor. Table 1 provides the categorization of the actors according to the CBL model. External data sources can be data controllers or data processors depending on the relation to the actor hiring their services. For example, if an external data source service (e.g. a Third Party Service) is hired by a data controller, then the external data source service provider will be considered as a data controller.

### Legal Analysis

Introduction of new services and technologies for data sharing and transfer entails the need to frequently re-evaluate the various risks and threats to patient's sensitive data and implement necessary e-Authentication and e-Authorization measures to counter them. In this use case, the patient personal data is uploaded on an e-Authentication/e-Authorization platform securely through adequate procedures, depending on the level of data sensitivity. It is assumed that the e- Authentication/e-Authorization platform authenticates and authorizes each user and provides access to specific patient data.



### Categorization of Actors and Data Flow

All the actors in this use case have been categorized into data subject, data controller, data processor and Third party for ease of legal analysis. The patient has been categorized as the data subject who owns the personal data. Service provider, field representative, external data source and AAL service providers have been categorized as data controllers. The electronic platform, databases, external data source as well as the AAL service providers have been categorized as data processors.

**Table 1: Data Roles of Actors**

<i>Actors</i>	<i>Data Subject</i>	<i>Data controller</i>	<i>Data processor</i>	<i>Third Party</i>
Patient				x
Field Representative/ Service Provider				x
AU2EU e-Authentication/e- Authorization platform				x
Database service providers				x
External Data Sources				x

### Mapping Actors and data to regulations

Figure 5 portrays the mapping of the patient registration use case specific actors to their respective legislation and regulations. Each actor of the use case has been mapped to the regulations they are bound by. Corresponding regulation articles have also been presented. More details of the mapping of actors like data subject, data controller, data processor and third parties to the legal legislations are provided in the regulation document pertaining to electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [5].

### VI. Conclusion

This combined business and legal framework will provide guidance to organizations in identifying the responsibilities and liabilities of the parties involved in a business process, notably aimed at (public) public health data exchange related issues. This combined business and legal framework has some noteworthy contributions.

Firstly, the framework ensures that approaches to electronic data privacy and security balance the underlying risk with the need for ease of use on behalf of all parties involved.

Secondly, it enhance confidence of parties (government or private) in electronic dealings.

Thirdly, it provides consistency in processes for electronic data security and privacy through authentication and authorization in order to increase efficiency.

Additionally, it also provides agencies with the tools to determine the most appropriate approach to the data privacy and security in a business process.

Finally, it can be used for ensuring application of due diligence when determining authentication and authorization approaches.

### **References**

- [1] I. Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe," *International journal of medical informatics*, 52, 105-115, 1998.
- [2] B. Stanberry, "The legal and ethical aspects of telemedicine," *Data protection, security and European law. Journal of Telemedicine and Telecare*, 4, 18-24, 1998.
- [3] Van Lamsweerde A., "Elaborating Security Requirements by Construction of Intentional Anti-models", in *Proc. ICSE'04, 26th Int. Conf. On Software Engineering*, Edinburgh, ACMIEEE, May 2004 [2] *Security, Amendment 11 of Annex 17, ICAO*, November 2005
- [4] R. Darimont, M. Lemoine, "Goal-oriented Analysis of Regulations" *ReMo2V*, 2006.
- [5] A. Refaut, C. Feltus, "Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach". *ReMo2V*, 2006.
- [6] Cousins J, Stewart T. *What is Business Process Design and Why Should I Care?*. RivCom Ltd. 2002 Apr.
- [7] Regulation (EU) 910/2014, OJ L 257, 28.08.2014, p. 73–114 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC".