# Centralized Management of Medical Big Data in Intensive Care Unit: A Security Analysis

Theodoros Mavroeidakos[†*], Nikolaos Tsolis[*] and Dimitrios D. Vergados[*]
[†]School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece
[*]Department of Informatics, University of Piraeus, Piraeus, Greece
[†]el10807@central.ntua.gr,[*]{tsolis,vergados}@unipi.gr

***Abstract*—The digital evolution of computing environments has affected the collection and management of medical data. Since there is a constantly growing number of remote sensors and medical systems, which augment the volume of medical data, a new challenge about the management of these big data is created. As the legacy systems in effect do not have the ability to manage this rate of data efficiently, it is of great importance to address this challenge following a different approach. In this particular unit of hospitals, ICU, the usage of complex medical systems in order to provide adequate quality of healthcare services and the velocity of the decision making process, which is performed by intensivists, are critical. To this end, an approach to this problem constitutes the Centralized Management (CM) of medical data in Intensive Care Unit's(ICU) environment. The autoscalling computing environment, which will be orchestrated in the context of operations of the CM will ease tasks, such as the aggregation of medical data by different sources, the performance of analytic functions and it will enhance the intensivists' cognition. Moreover, this type of management leads to security and privacy challenges that should be addressed in order to assemble a highly trusted environment both in technical and functional level. As a result, prior to the adaptation of the CM in ICU, specific security, as well as privacy guidelines, should be determined.**

***Index Terms*—Centralized management; medical big data; intensive care unit; security challenges; security guidelines.**

## I. Introduction

The big data environment, as defined in [1], is characterized by five dimensions namely the volume, the velocity, the variety, the value and the variability. This type of environment is highly associated and compatible with the idea of the CM of data. Moreover, many sub-challenges exist due to the scale and type of data sets which create the superset of medical big data. In particular, the collective rhythm of data by the EHR record systems, genomic information, remote sensors and mobile devices are amplified constantly. As a result, the computing environment in this approach should be constructed based upon the five dimensions of any big data environment. Accordingly, the first objective is to design a cyber-infrastructure accommodating medical data and integrating the in-hospitals legacy systems in order to provide enhanced operations concerning the data such as capture, analysis and visualization. Thus, this infrastructure will be distributed and it will be based upon a cloud environment with characteristics such as the elasticity and the scalability. However, the distributed environments, due to their structure, are threatened by a wider spectrum of attacks and as a result the vulnerability management will be of paramount importance. Also, the ICU consists a critical medical sector, because of the variety and the volume of medical data that are processed in order to provide healthcare services. Furthermore, in a medical unit, the response time to face or prevent a medical event is crucial. The CM will enable to intensivists the ability to access real-time as well as of past data of any admitted patient directly so as to support any decision concerning their treatment. Due to the sensitive nature of medical data, which will be collected, processed and managed such as demographics as well as data related to the medical condition of any patient, the CM should be characterized by a high level of security and privacy.

The rest of the paper is organized as follows: In Section II the related research literature is reviewed, while Section III contains analysis of functional and clinical operations in ICU. Section IV contains the description of medical big data which will be managed by the proposed type of management. Section V consists of major points of interest which are of high importance during the development of a secure centralized management. Section VI consists of the performance evaluation while conclusions are drawn in section VII.

## II. Related Work

Addressing the adoption of centralized big data environment in ICU, it is necessary to revise the research literature, as well as implementations that have been orchestrated so far concerning medical big data.

According to [2], the problem of big data on intensive care units of Francisco Lopez Lima Hospital is identified and the medical equipment, which is necessary so as to collect the physiological data of patients, as well as, the underlying cyber-infrastructure that supports the management of data is described. The proposed approach consists of an architecture, which is based on a scalable system such as a cloud computing environment in the context of which the aggregation of data and effective operations on big data are performed. Belle et al. [4] argue about the research made on clinical decision support systems based on big data technology. Moreover, the study, which is presented in [5], describes the prediction and prevention of medical incidents based on a scalable infrastructure that assists the collection and analysis of physiological data in real time. The Artemis system which is presented in [6], is based on a health platform that supports real time analysis of parallel physiological data streams. The Artemis system deployed at first in the neonatal intensive care unit at the

978-1-5090-4476-4/16/$31.00 ©2016 IEEE

hospital for Sick Children in Toronto. According to [7], the information strategy which uses big data should be created by following five specific steps namely the definition of all data sources, the setup of data quality metrics, the integration of data sources, the identification of analytic needs as well as the security and management of the data lifecycle. Katehakis et al. argue in [8] about a distributed agent-based architecture for the acquisition, management, archiving and display of real-time monitoring data in the ICU that makes efficient use of the Common Object Request Broker Architecture (CORBA).

The aim of this study is to analyze the functional operations as well as the practices and guidelines of a centralized information management system in the context of operations of the ICU. This clinical information system (CIS) will coordinate the workflow inside the ICU and it will improve the quality of the provided healthcare services. The ultimate goal of the CM is about accomplishing computerized patient charting. The proposed paperless type of management takes into consideration the fact that the adoption of such a system by the nursing staff, as well as the intensivists, will be a challenge.

## III. Analysis of Work Flow in ICU

During the length of stay in ICU, healthcare services are provided to patients with critical care needs who require highly specialized equipment and expertise. The mission of ICU is the uninterrupted monitoring of critically ill patients, who suffer from malfunction or failure of individual organs and in many cases of entire organ systems. The ICUs in Greek hospitals consist of 8-10 beds and for every bed 4-6 medical devices support the medical condition of each patient. Following the admittance process, the intensivists and the nursing staff share a special form concerning the treatment of the patient. Specifically, doctors fill in their instructions according to the patient condition. Due to the fact that the patients are critically ill, the nursing staff shall complete the arrangement of the initial medical processes in a specific period of time. Then, the nursing staff use the instructions to monitor and log data to medical documents. These data are vital signs, such as the temperature and the arterial blood pressure which are manually logged every hour within a full day of twenty-four hours. At first, they set the appropriate amount of serum and its type that is needed to flow through installed pumps and have medicines dissolved into serum. Further, the nursing staff administer nutrition and fluids to the patient through the Levine tube and log medicines which are infused to patients. Finally, in case of any medical incident with regard to the condition of the patients, the nursing staff may log emergency notes.

## IV. Medical Big Data

The medical big data are classified into four types of categories: *the blood type, the respiratory type, the blood gases type and the waste fluids type*. *Blood and respiratory type of data* as well as data concerning blood gases are handled by both the doctors and the nursing staff, while data about the waste fluids are processed only by the nursing staff. According to specific timetables the data measurements are performed by the nursing staff into medical documents which are examined by the intensivists. The *blood and respiratory type of data* are the main categories of data which are targeted by a wide spectrum of sensors and wearable devices able to communicate with a cyber-infrastructure independently without human interaction.

In the category of the *blood type data*, specific measurements are made. The central arterial and intra-abdominal pressures (CVP/IAP) are extracted from monitor indications. The Positive Airway Pressure/Pulmonary Artery Occlusion Pressure/Static Compliance (PAP/PAOP/CStat) are airway pressures, which and are extracted from ventilator and monitor indications. The ICP/PtiO2, which are intra-cranial pressure and partial brain tissue oxygenation that are extracted from monitor indications. The Na/K/Cl and Glu are blood electrolytes, which are collected from the blood gas analyzer, a clinical system, which collects blood samples from patients.

In the category of *respiratory type of data*, a special notification which shall be made, is about the ventilation mode (supported, assisted, self-sustaining breath) of the mechanical ventilation which supports each patient. Different data measurements of the respiratory type are made according to each ventilation mode. The Fraction of Inspired Oxygen (FiO2) is the amount of oxygen infused into the ventilator. The saturation of oxygen in blood (SaO2) is measured from the patient's fingers with a technique called oximetry. The result of this technique is displayed in the monitor. The Respiratory Rate (RR) of the patient is adjustable in the ventilator. The Tidal Volume (VT) is the volume of each breath and it is also adjustable in the ventilator. The Positive End-Expiratory Pressure (PEEP) is the pressure developed at the end of exhalation and it is adjustable in the ventilator. The RR, VT and PEEP are adjusted by the nursing staff according standard medical instructions by the doctors of ICU.

The current situation in the context of operations of ICUs is that the nursing staff log measurements of vitals in specific intervals of time into medical documents. Also, the Clinical Information System (CIS) of ICU assists mainly its functional operation without supporting its medical operations.

## V. Centralized Management Development

The CM will provide better quality of services including attributes such as stability, capacity, performance tuning, availability, disaster recovery, usability and security. These characteristics would be embedded into the ICU-oriented CIS by the big data application of the CM providing a rich set of features. These features involve equipment monitoring with regard to the patients condition, accumulation of the patients data which lead to the creation of Electronic Health Records (EHR) and automatic analysis of data by following statistical models. Moreover, the intensivists will acquire the capability to perform diagnosis remotely by using collections of data for each patient as presented in Figure 1.

The functional units of the CM include the management of EHR and actions performed by the nursing staff, the operations of the ICUs administration, the ICUs resources, the support of telemetry and radiology information systems as well as imaging examinations and finally the management of the medical library of the ICU. Despite the benefits of the CM in ICU, an integration methodology as presented in Figure 2 shall be followed so as to incorporate it in the work-flow of this medical unit.

### A. *Cyber-Infrastructure Apparatus*

The cyber-infrastructure of the CM enables the adoption and promotion of Wireless Sensors Networks (WSNs) and Body Area Networks (BANs) in the ICU despite the clinical systems already in use. These sensors will improve the capabilities of the clinical medical systems by performing measurements about health rate, non-invasive blood pressure, invasive blood pressure, arterial oxygen saturation, pulse rate, respiration rate and body temperature. The main problem that exists in those networks is the quantity of real-time data streams, which are collected. The solution lays on the underlying infrastructure supporting the storage and management of physiological data. The web-application of the CM is supported by a scalable system, able to increase its storage and processing power in real-time in order to handle the capacity of data. The web-application collecting the transmitted data by the sensors is supported by software alarms with scope to trigger specific *scaling policies*, which in turn will deploy a dynamic number of physical resources in order to satisfy the storage capacity as well as the network traffic.

The cyber-infrastructure is a cloud computing (CC) environment, constructed according specific security specifications. Thus, an appropriate load-balancing system will be employed alongside the CC *Availability Zones* in order to achieve a high level of availability. By appropriately configuring the *Availability Zones* and supervising their deployment, they shall be utilized as a defensive mechanism against certain types of attacks (i.e. DDoS attacks). Moreover, due to the CC environment, security groups, which act as virtual firewalls will be orchestrated in order to control with their rules the inbound and outbound traffic, which reaches the availability zones and their entities. Thus, it is crucial to construct a policy, which will supervise the configuration of the CC security mechanisms. The *Availability Zones* are auto-scaling groups consisting of *Instances*. The *Instances* are virtual entities of web-servers which support the provision of the end-service. To this end, the environment is characterized by elasticity and scalability as well as a high level of availability. As presented in Figure 3, the nursing staff and the doctors will interact with the application of CM, as well as the communication between the medical sensors and the cyber-infrastructure will take place through an access point or base station.

### B. *Policy*

The policies will engage with the terms of usage of the medical big data as well as any information which is generated by the diagnosis procedure. The collection, analysis and retention of data will follow the national regulations concerning the processing and protection of personal data as the medical data will be processed by automated means. By incorporating a minimum access policy, the nursing staff and the intensivists will use the application of the CM under predetermined occasions and by following specific rules. A policy of acceptable use will be orchestrated in order to define the borderline between the acceptable actions and the unacceptable, which will be prosecuted. Due to the fact that there will be terminal stations in ICU, which will facilitate access to the environment of CM, a password policy will be embodied also.

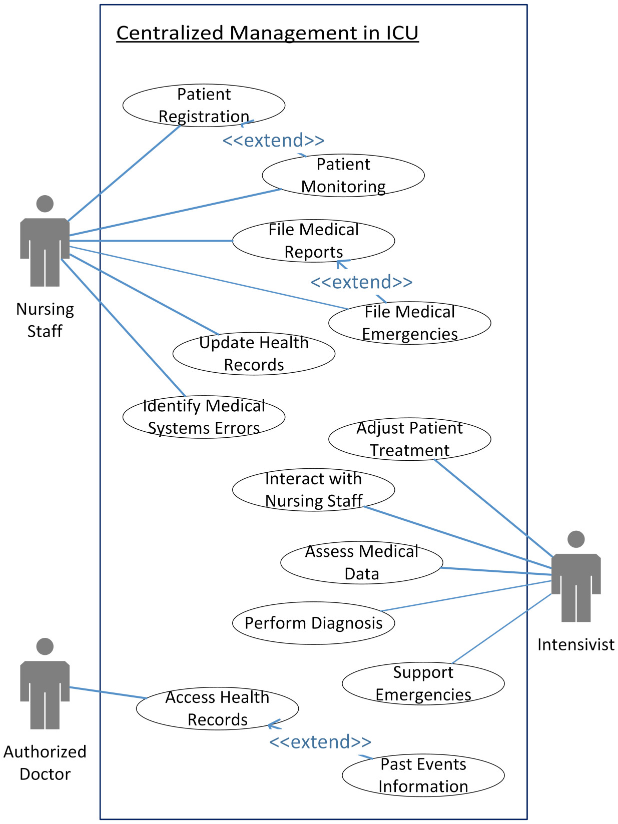


Fig. 1. Use Case Diagram of the Centralized Management.

### C. *Privacy and Ethics*

According to [9], the CM will consist of three major aspects concerning the privacy of patients with regard to their Personaly Identifiable Information (PII) and the moral principles, which will define its ethic perspective. These points are namely the *(a)* informed consent processes, *(b)* privacy practices and *(c)* legal compliance. In the context of informed consent processes, the applicant will grand access to his ePHI unambiguously and as a result the functional as well as the clinical operations will gather data appropriately. The privacy practices are about the concept of implementation of policies and procedures with regard to authorization, access controls and permissions of specific functions such as capture and analysis of medical data.

In the context of the privacy practices, the project coordinator of the CM shall be able to articulate the reasons upon,

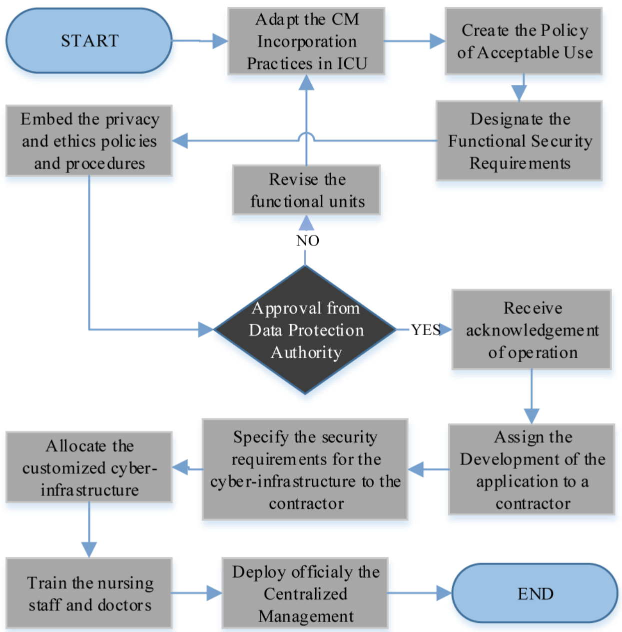


Fig. 2. Integration Methodology of the CM in the ICUs' work-flow.

which the data are collected and are processed. This situation will ease the task of authoring the privacy documentation and analyzing privacy compliance issues. The privacy compliance documentation is substantial to be completed prior to the deployment of the application, which will gather PII with regard to the CM. This type of documentation will be based on a standardized compliance document such as the Privacy Threshold Analysis (PTA) or the Privacy Impact Assessment (PIA). The privacy objectives, which will govern the implementation of the CM and its actions on the cyber-infrastructure, as well as the authoring of the documentation, are namely the transparency, the accuracy and the consistency. Moreover, the privacy policies also contain the classification of the medical big data collected in ICU into explicit categories. To this end, the personnel of hospitals' workforce acquire access in those categories according to its duties. In order to ensure that access is obtained in the context of specific terms, a code of conduct shall be employed.

The CM will operate according the Greek National Law 2472/1997 regarding the processing and securing of personal data, which was formed by the *European Data Protection Directive 95/46/EC*. Moreover, a long-term objective in eHealth is interoperability, which will be incorporated in the operation of the CM by engaging with the article 14 of the *European Cross Border Healthcare Directive 2011/24/EU*. The guidelines, which will structure the informed consent processes and the privacy policies, will be based on articles of the national law related to the purposes of process as well as the concept of liabilities. The operation of the CM will be authorized and supervised by the Hellenic Data Protection Authority (HDPA), which also shall approve the legality of this type of management and it will determine the adequacy of the provided level of security. The legal requirements surrounding the processing and securing of personal data will guide the incorporation and configuration of the technical environment.

### *D. Security*

A formal security plan based on security standards and safeguards shall be completed prior to the development of the application of CM in ICU. Thus, security by design will be followed from the beginning. This specific plan will be formed by the Confidentiality, Integrity and Availability (CIA) principle and it will be incorporated into the functional as well as the technical level of the CM [10]. The CM by following practices concerning the Confidentiality will preserve the privacy of PII and medical data collected and processed during its operation. With regard to Integrity, the collected data in this custom cyber-infrastructure will be managed transparently without tampering with them. To this end, certain security policies will govern the authentication as well as the authorization of actions which are performed by the nursing staff and the intensivists. Moreover, it is crucial that monitoring mechanisms shall be activated, in order to identify unauthorized actions as well as human errors. According to Availability, medical decisions and actions, which are performed in the context of the CM as well as electronic Protected Health Information (ePHI) will remain available regardless of any threatening incident to the operation of the cyber-infrastructure. Also, regarding the availability, the cyber-infrastructure hosting the web-application of the CM, shall be supported by adequate redundant systems so as to resolve physical outages or cyberattacks without affecting the performance of ICU. Further, due to the sensitive nature of PII such as demographic information, ePHI and medical decisions concerning the treatment of admitted patients, the defensive mechanisms shall operate in the context of security objectives such as the reliability and the confidentiality. These security objectives will form the security and privacy level under which the management operations will take place. Further, the security plan shall contain risk management actions so as to identify and prevent threats against central points of failure such as the terminals, which will allow access to the cyber-infrastructure and they will be managed by the nursing staff. As a result, the nursing staff shall be trained concerning security and privacy threats so as to identify and report any cybercriminal activities with regard to PII.

## VI. Performance Evaluation

The evaluation of the CM performed in the context of collecting PII during the treatment of a patient in the environment of ICU. The pilot implementation of the CM conducted in the General Oncology Hospital of Kifissias in Athens. Having already integrated the CM in the ICU, data measurements were collected in the context of ICU's clinical operations for one weeks' period from one patient. The data measurements involved medical measurements, which were appointed by a daily clinical schedule, as well as medical laboratory and imaging examinations, which were arose by

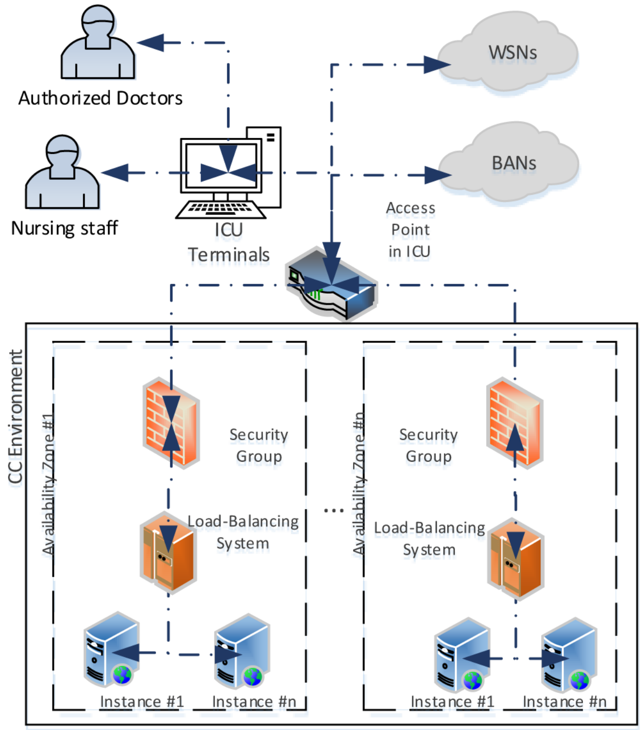


Fig. 3. Cyber-Infrastructure of Centralized Management

the medical condition of the patient. Figure 4 presents a comparison between the collected *Gigabytes per Day* by the underlying environment of CM and a legacy environment. As identified, the CC environment facilitates features, which enable the collection of data by internal and external sources in multiple formats. Moreover, the communication between sensors and the CC environment allows the collection of a diversity of medical data in strict intervals due to the available capacity of storage. During the evaluation, the orchestrated security measures did not pose any performance constrain.

## VII. Conclusions and Future Work

The CM brings many benefits in the operation of ICUs. By adopting the CM in the ICU, the QoS of healthcare services is improved. This improvement occurs due to the management and analysis of huge data sets, which assists the decision making process followed by the doctors and nursing staff in the context of treatments. However, many issues concerning the level of privacy and security of CM should be addressed due to the collection of personal data prior to its deployment. Moreover, the CM solves the problem of the identification of human errors due to the strict supervision of the medical actions. The CM is only limited because of challenges such as the training of nursing staff and doctors.

Due to the level of performance and security, the adaptation of CM in Greek and European hospitals, consists of a solution of high importance. Beyond its benefits, CM enables the integration of systems, which will take advantage of the centralized data collection so as to increase the cognitive capabilities of doctors. To this end, machine learning algorithms are capable to perform analysis of complex medical data by utilizing statistical models so as to predict values, which will accelerate and improve the clinical work of intensivists and subsequently, the QoS of medical services is enhanced.

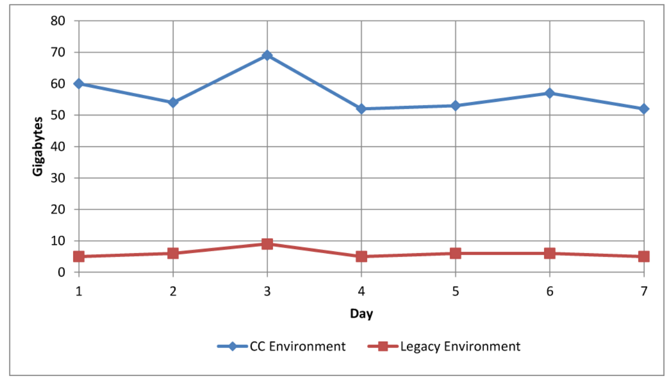


Fig. 4. Medical big data aggregation for one weeks' period

## Acknowledgment

The publication of this paper has been partly supported by the University of Piraeus Research Center (UPRC).

## References

[1] W. Fan and A. Bifet, *Mining Big Data: Current Status, and Forecast to the Future.* SigKDD Explorations, 14(2), 2014, pp. 1-5.

[2] J. Balladini, C. Rozas, E. Frati, N. Vicente and C. Orlandi, *Big Data Analytics in Intensive Care Units: Challenges and applicability in an Argentinian Hospital.* Journal of Computer Science & Technology, 15(2), November 2015, pp. 61-69.

[3] A. Belle, R. Thiagarajan, S.M. R. Soroushmehr, F. Navidi, D. A.Beard and K. Najarian, *Big Data Analytics in Healthcare.* BioMed Research International, 15(1), 15 June. 2015, pp. 1-16.

[4] A. Belle, M. A. Kon and K. Najarian, *Biomedical informatics for computer-aided decision support systems: a survey.* The Scientific World Journal, 13(1), 9 January 2013, pp. 1-8.

[5] H. Han, H. C. Ryoo and H. Patrick, *An infrastructure of stream data mining, fusion and management for monitored patients.* 19th IEEE International Symposium on Computer-Based Medical Systems, Salt Lake City, Utah, USA, June 2006, pp. 461-468.

[6] M. Blount, M.R. Ebling, J.M. Eklund, A.G. James, C. McGregor, N. Percival, K.P. Smith and D. Sow, *Real-Time Analysis for Intensive Care: Development and Deployment of the Artemis Analytic System.* IEEE Engineering in Medicine and Biology Magazine, 29(2), March-April 2010, pp. 110-118.

[7] IBM Software, White Paper, *Data-driven healthcare organizations use big data analytics for big gains.* February 2013, pp. 1-7.

[8] D. G. Katehakis, G. Chalkiadakis, M. Tsiknakis and S. C. Orphanoudakis, *A Distributed, Agent-Based Architecture for the Acquisition, Management, Archiving and Display of Real-Time Monitoring Data in the Intensive Care Unit.* Foundation for Research and Technology - Hellas, Institute of Computer Science, Technical Report 261 (FORTH-ICS/ TR-261), Heraklion, Crete, Greece, October 1999.

[9] Experts Working Group on data protection and privacy, *Data protection and privacy ethical guidelines.* Ethical Review in FP7, European Commission, September 2009, pp. 3-18.

[10] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith and D. I. Steinberg, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.* National Institute of Standards and Technology (NIST), NIST Special Publication 800-66 Revision 1, 2008, pp. 6-25.