Trust Management Framework For Iot-Based Ad-Hoc Patient-Monitoring Medical Devices In Critical Care Areas

Raghu Nallani Chakravartula, Dr.V.Naga Lakshmi

Abstract: With the rapid advancements in the mobile, electronics miniaturization, Web, and wireless technologies, the computing environment is seamlessly getting integrated into the everyday objects in the physical world. The proliferation of these smart objects connecting to the Internet leads to a novel paradigm called the "Internet of Things (IoT) or "Internet of Everything (IoE)." It has been widely accepted that our daily lives will be fundamentally enriched with IoT-based medical devices. Along with the incredible opportunities provided by IoT, it also opens new security risks and privacy threats. The paper proposes an innovative approach for trust management framework for patient monitoring healthcare devices in critical care areas at hospitals.

Keywords: Human-notion of trust, Authentication, and Authorization, peer-to-peer network, Internet of Things (IoT), Patient monitoring medical device and application.

1 INTRODUCTION

In IoT space, everyday objects are equipped with microprocessors for data acquisition, transceivers to enable them to sense the environment and communicate with each other over the Internet [1]. The IoT involves distributed nature, pervasive presence with heterogeneous devices. In this environment, intelligent objects can communicate with one another forming a promising model to offer services that can be accessible to anyone, anywhere, anytime [2] Hence, the Internet of Things is going to be the next game changer that promises to transform the way we live, work, play and learn. Internet of Things may redefine social, economic and technical elements in many sectors with accelerated growth resulting in innovative and novel applications. The large-scale implementation of IoT devices brings tremendous opportunity with disruptive applications. In such an environment, security of the applications and privacy of the users are the major barriers for the penetration of IoT-based Medical devices. Traditional authentication and authorization solutions do not meet the requirements of IoT-based resource constraint devices and pose limitations and patient safety issues.The proposed authentication and authorization framework dynamically perform trust negotiation to allow or reject permissions and actions among devices [3]. The paper presents various scenarios in patient monitoring medical devices with Hexagon framework and shows the analysis details. The proposed trust negotiation framework evolves trust dynamically using six important parameters, and they are as follows Privacy, Identity management, Reputation, Peer recommendation, Operational Cost, Operational Risk. Having given introduction and motivation of the work, the rest of this paper is organized as follows. Section 2 presents the related work. Patient monitoring of vital parameters and medical sensors are described in section 3. The proposed architecture of the Hexagon framework is described in section 4. Section 5 provides a deployment model and various scenarios in trust negotiation among devices. Conclusion and future work is captured in section 6.

- *Raghu Nallani Chakravartula is currently working with Astro Malaysia Holdings Berhad, PH-+60-128004020. E-mail: raghunc@gmail.com*
- *Dr.V.Naga Lakshmi is currently working in Gitam's University as Professor, India, PH-+91-9573569913. E-mail: nagalakshmi.vadlamani@gmail.com*

2 RELATED WORK

Trust management framework is studied at great details by various projects. Some of the key project details are as follows –Simple Universal Logic-oriented Trust Analysis Notation (SULTAN) [4] is a trust management framework that allows the user to specify, analyze and maintain and manage the relationship between several entities. The framework allows to manage all the policies at the centralized server and is inappropriate for ad-hoc objects. Policy Maker [5] is considered the oldest framework for peer-to-peer based distributed trust management. It makes trust decisions based on static rule-based policies. However, trust negotiation is dynamic, and the decision has to be evaluated on the fly based. Therefore, this approach is not suitable and has limitations in trust evaluation.

Other similar projects are "Supporting Trust in the Dynamic Establishment of peering coaLitions" (STRUDEL) [6], "Secure Environments for Collaboration among Ubiquitous Roaming Entities" (SECURE)[7], "Human Trust Management Model and Framework" (hTrust) [8], "Risk-Aware Decision Framework for Trusted Mobile Interactions" [9], , and "Trust Based on Evidence" (TuBE)[10],[11]. All the above frameworks are focussed on dynamic trust negotiation but fail to capture the parameters that influence the human notion of trust. Also, the above frameworks are targetted for generic applications and cannot be applied to healthcare medical devices. Considering the European Union privacy laws [12], GDPR [13] and HIPAA [14] compliance, the above frameworks lack design control to preserve the privacy of IoT-based medical devices. The proposed Hexagon framework addresses the above limitations by authentication and authorization the IoT-based peer-to-peer patient monitoring smart objects by capturing trust and privacy dynamically with no user intervention.

3 PATIENT HEALTH MONITORING AND IOT

The ultimate goal of every medical facility is to improve the patient's condition or at minimum ease their suffering [15]. Internet of things helps by providing solutions, which generate detailed patient information and make it readily available over the Internet to right stakeholders, necessary to make rapid and accurate decisions by the panel of doctors in order to achieve the best patient outcomes. The research is focused on securing IoT based medical devices used in life care support of patients in critical care areas like transport, Emergency Departments (ED), Intensive Care Units (ICU), Surgery departments, cardiac diagnostic centers, newborn nursery centers, labor and delivery centers, etcTo achieve the best possible outcomes in the patient's health condition, monitoring of critical parameters is essential. Monitoring may occur on an intermittent basis, such as having the blood pressure checked during an annual physical examination or in a continuous manner such as monitoring breathing when anesthetized during an operation. The Internet of Things plays a critical role in the diagnosis monitoring and treatment of the patients. Technology helps to synthesize the data obtained during monitoring, with the patient's condition, past medical history, and diagnostic study results.[16] Patient's vital parameters are merely the measurements of vital bodily functions. The determination of which parameters to monitor varies by patient condition. In some cases, the monitoring processes are painless and take seconds. Other parameters require invasive procedures to place tubes, sensors, and probes within the heart, vessels, and lungs. Invasive procedures result in an increased risk of injury or infection for the patient and typically are more expensive. The physiological data available is compared to normal limits, to make emergent and long terms decisions in the care of the patient. Rarely data points are taken into consideration in conjunction with other patient assessment data such as level of consciousness, pain, and the patient's past and current medical history. A drastic change in a parameter will generate an alarm and cause concern; fortunately, it does not always mean the patient's condition is deteriorating. The alarm signals the need to check on the patient. Patients have been known to remove electrodes or disconnect themselves from the monitoring devices when confused or agitated, in order to go for a walk or go to the bathroom. False alarms also occur. While universal levels of normal are already established, alarm limits (high and low), as well as alarm priorities, may vary from organization to organization. IoT-based patient monitoring sensors and Actuators are used to measure vital patient parameters. An IoT-sensor is a module, device or subsystem used to detect events and changes in its surrounding environment and trigger the information to the processing unit. An Actuator is a module of the system that is responsible for controlling and moving a mechanism or system. It requires a control signal and source of energy. The actuator is responsible for converting the signal energy into mechanical motion. There is a wide array of sensors and actuators available to measure or detect changes in patient monitoring. The below figure 1 shows the list of sensors used for detecting the vital parameters of patients and table 1 describes the respective details of each sensor used in this study [17]

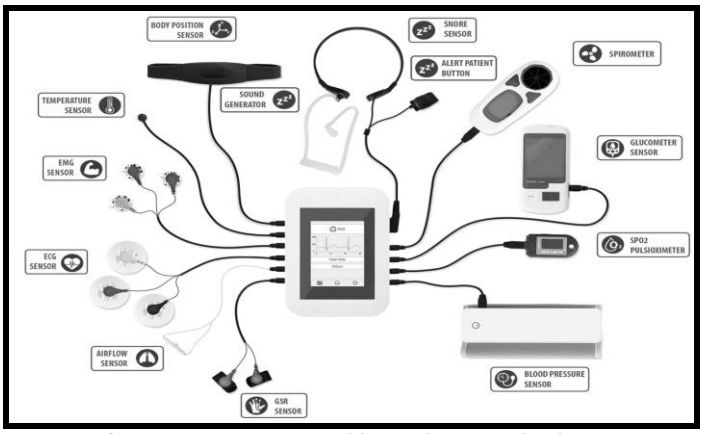

Figure 1 *Sensors used in Patient monitoring*

SENSOR DIAGRAM	DESCRIPTION
	Snoring is the loud and unpleasant sound during sleep. It is caused due to obstructed air movement due to vibration of respiratory structures while sleeping. Snoring is the initial sign of obstructive sleep Apnea (OSA) and one of the primary factors of sleep deprivation. The sensor allows measuring the vibration of respiratory structure to determine the severity of snoring.
	Human body temperature is a primary part of the clinical examination. A change in body temperature is the first alarm for indication of the health of the patient. Body temperature plays a vital role in the newborn. The sensors allow measuring the body temperature accurately.
	Galvanic Skin Response or GSR for short is a mechanism to measure emotions and sleep quality. Emotions will cause a stimulus to the nervous system resulting in sweat secretion. The sensor is used to identify strong emotions with the electrical conductance of the skin. The sensors work by attaching it to two fingers of the same hand to measure the electrical conductance.
	Glucometer sensor helps in determining the concentration of glucose levels in the blood. It works by placing a drop of blood on a disposable strip, and the sensor will be able to determine the blood glucose levels. Glucose in the human body is the primary source of energy and is regulated with insulin (a hormone produced by the pancreas). Change in glucose levels compared to normal healthy values result in a wide array of complications.
	The electrocardiogram (EKG or ECG) is a diagnostic procedure to determine the health of the heart. It assesses the electrical and muscular functions of the heart by placing the electrodes over the skin to measure the electrical activity over a period.
	An electromyogram (EMG) is used to assess the electrical activity of muscles at rest and during contraction. An electromyogram acts as a diagnostics tool for identifying neuromuscular diseases, assessing kinesiology, low-back pain, and disorders of motor control. EMG signals are also used in many biomedical applications. This sensor will assess the rectified and filtered electrical activity of a muscle to determine the amount of activity in the muscle such as prosthetic hands, arms, and lower limb, etc.

	A spirometer is an apparatus for measuring and determining the volume of air expire and inspired by the lungs. A spirometer is used to measures the movement of air into and out of the lungs and ventilation. The apparatus will be able to identify two different types of abnormal patterns - obstructive and restrictive. The sensor uses pressure transducers to find the cause of shortness of breath, and it helps doctors to find lung diseases such as asthma, emphysema, bronchitis.
	Pulse oximetry is a non-invasive method of monitoring the oxygen saturation (SPo2) levels. Pulse oximeter allows measuring the SPO2 levels by light-emitting diodes facing a photodiode through a translucent part of the finger.
	Blood pressure (BP) is the pressure in large arteries or by circulating blood on the walls of blood vessels. This sensor measures BP non-invasively using mercury-tube sphygmomanometer.
	The airflow sensor used to measure the breathing rate in a nasal / mouth airflow of the patient. The sensor consists of a set of two prongs to be placed in the nostrils and thread to tie behind the ears to hold the device over a period.
	The human body parameters vary based on the patient's position and posture. The accelerometer sensor monitors patient positions like standing, sitting, supine, prone, left or right. It uses a triple axis accelerometer to obtain the patient's position.
	Weighing scale sensors helps to measure the weight of the patient or to measure the mass of the patient. It helps to measure body fat, bone mass, muscle mass, body mass index, body water, visceral fat, basal metabolic rate.

***Table 1 Patient** Monitoring Sensor and description*

4 HEXAGON FRAMEWORK

Trust negotiation plays a critical role in authentication and authorization of ad-hoc objects in the distributed network due to lack of centralized service. The objective behind the trust negotiation framework is to represent the human notion of trust in terms of computational algorithms for IoT-based ad-hoc patient monitoring devices. The decisions are solely taken by evaluating trust decisions between or among objects without minimum to no human intervention to closely resemble how trust happen among the individuals in the physical world. Hexagon framework proposes six important parameters to arrive at trust value and hence it is named "Hexagon Framework." The six parameters are Privacy, Identity management, Reputation, Peer recommendation, Operational Cost, Operational Risk used for representing and deriving trust among objects. Peer Recommendation: Recommendations are solicited from peers, and it helps in making trust decisions. Privacy: Privacy decisions are made based on the user choices defined by each user in this component. Operational Cost: The component determines the cost involved in performing an action. It considers actions like bandwidth used, battery power and processing required, etc. to allow or reject permission to perform a particular action.

Operational Risk: Cost-benefit analysis is performed in this component to evaluate the risk involved by performing a particular action.

Reputation: The rating provided by peers are used to arrive at trust decisions. Past interactions are stored in the database.

Role and Identity Management: This component allows the user to use pseudonyms to allow anonymous access to resources to ensure the privacy of the user.

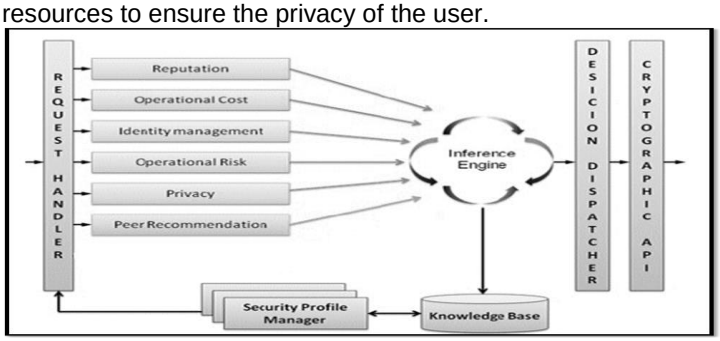

***Figure 2** HEXAGON Framework and various modules*

The following are the components of Trust management framework as depicted in figure 2

4.1 Request handler: Request handler acts as a façade to allow external requests and forward to the six modules to determine trust calculations.

4.2 Security Profile Manager: Security Profile manager acts like a Graphical User Interface (GUI) that allows configuring the smart object for the first time

4.3 Knowledge Base: Knowledgebase allows to store the configuration settings and values of endpoints and acts as a data store.

4.4 Inference Engine & Decision Dispatcher: Interface engine is the heart of the framework. Trust negotiation is evaluated using fuzzy logic for the: computation of trust value obtained from each module. The component dispatches the final trust value and stores in the database for future decisions and uses cryptographic interface to send trust decisions.

5 DEPLOYMENT OF HEXAGON FRAMEWORK IN PATIENT MONITORING

Trust Management Framework receives the request from a peer-to-peer application through a request handler for negotiating the trust value. Each component provides its respective computed value to the inference engine for evaluating and calculating the final trust value. Configuration options stored in knowledge store is retrieved to evaluate pass interactions and user privacy preferences while making the decision. The request handler uses the preferences set in the profile while computing the trust value. The final decision is dispatched to the application. Hexagon framework has been tested on patient monitoring devices in critical care areas at hospitals. The framework allows the sensors of patient monitoring to take trust-based decisions without human intervention as depicted in figure 3.

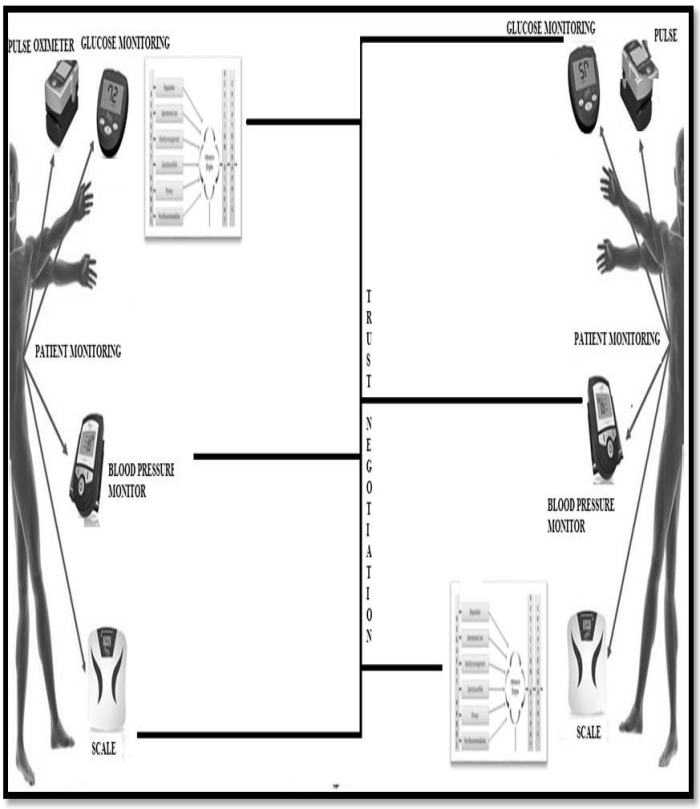

Figure 3 *Trust negotiation between patient monitoring devices*

6. ANALYSIS OF RESULTS

The below scenarios are simulated using Hexagon framework and comparisons are made between traditional user authentication and authorization models to trust based model

Scenario A: Calibration, firmware, patches, and updates.
Sensors: Weight scale sensors
Description: Scale A negotiates the trust level with other Scale B in the same network. When successful it can download the calibration information, firmware, patches, etc. It helps the scales to stay up-to-date and accurate.
Scenario B: Gestation diabetes in pregnant mothers
Sensors: Blood glucose sensors
Description: Trust negotiation among blood glucose sensors to other IoT-based sensors like refrigerator or oven to understand the patients eating habits and Accurately measuring patient's Glucose after lunch, dinner, snacks, and breakfast at defined time intervals in cadence will help gestation diabetic mothers to plan their diet accordingly. The data will help the doctors to mitigate any future complications for mothers and to newborns.
Scenario C: Sleep apnea and other sleep-related disorders
Sensors: SPO2, Blood pressure sensor, Body position sensor
Description: Trust negotiation among SPO2, Blood pressure sensor, Body position sensors help patients to identify sleep patterns and discover any sleep-related disorders like sleep apnea.
Scenario D: Sports athletes to improve performance
Sensors: EMG and ECG patches, SPO2, blood pressure and body scale sensors
Description: Trust negotiation among EMG and ECG patches, SPO2, blood pressure and body scale sensors and continuous monitoring help sports athletes after a workout to evaluate the performance of athletes and enable them to improve in their workout.
Scenario E: Endocrine disorders
Sensors: Body Scale sensors, Glucometer
Description: Trust negotiation among Body Scale sensors, Glucometer sensors and continuous monitoring help patients with endocrine disorders to monitor obesity, diabetes, overweight, etc.
Scenario F: Asthma attacks
Sensors: Spirometer, SPO2 sensor, and airflow sensors
Description: Spirometer, SPO2 sensor, and airflow sensors talk to each to monitor respiration in patients to diagnose allergies that can lead to asthma attacks.
Scenario G: Alzheimer's and dementia issues
Sensors: Body Scale sensors, blood pressure, blood glucose, and oxygen sensors
Description: Successful trust negotiation among the Body Scale sensors, blood pressure, blood glucose and oxygen sensors help elderly to monitor for Alzheimer's and dementia issues.
Scenario H: Heart attacks
Sensors: SPO2, Blood Pressure, ECG with patches sensors
Description: SPO2, Blood Pressure, ECG sensors talk to each other to monitor hypertension, arrhythmia, and tachycardia to prevent heart attacks.
Scenario I: Anaesthesia allergies
Sensors: Anaesthesia sensors, SPO2, Blood Pressure, Temperature, Body position
Description: Trust negotiation among SPO2, Anaesthesia, blood pressure, body position, and temperature sensors can monitor patients current condition and prevent anaesthesia allergies.
The below graph presents the performance improvement using the peer-to-peer model in red color compared to the traditional client-server model in blue as shown in figure 4.

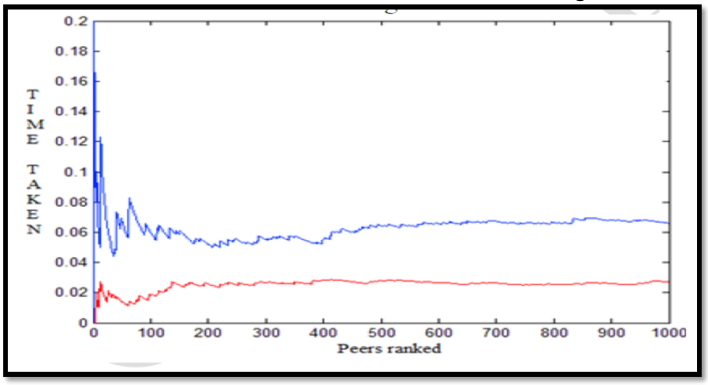

Figure 4 *Performance improvement using the peer-to-peer model Vs. client-server model*

The scatter plot for the association of interactions with malicious smart objects Vs. Interactions with trusted smart objects. The positive correlation shows the number of interactions with the malicious objects decreased over a period due to increase in the knowledge base database as shown in figure 5.

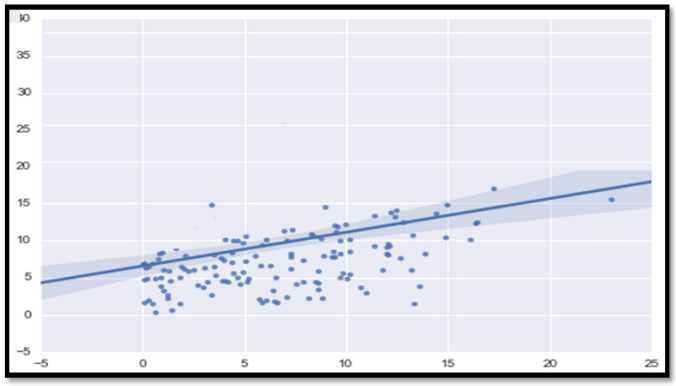

Figure 5 *Correlation coefficient graphs for interactions with malicious Vs. Trusted ones.*

7 CONCLUSION AND FUTURE WORK

This research presented the HEXAGON framework and demonstrated how Trust could be evolved among smart objects in an IoT-based environment. The study illustrates significant performance improvement by testing various real-world scenarios in patient monitoring and correlates the differences with malicious Vs. Trusted interactions in IoT-based healthcare devices in critical care areas at the hospital.

7.1 ACKNOWLEDGMENTS

The authors would like to thank General Electric (GE) Healthcare and Philips Healthcare support staff for helping us to measure, analyze and calibrate Patient healthcare monitoring sensors to experiment with various scenarios as part of this study.

7.2 REFERENCES

[1] Ashton K. That 'Internet of things' thing, RFID Journal, (2011).

[2] Dennis Gessner; Alexis Olivereau; Alexander Salinas Segura; Alexandru Serbanati, "Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things." (2012) IEEE 11th International Conference on Trust, Security, and Privacy in Computing and Communications, 2012

[3] Suneth Namal; Hasindu Gamaarachchi; Gyu MyoungLee; Tai-Won Um, "Autonomic trust management in cloud-based and highly dynamic IoT applications." (2015) ITU Kaleidoscope: Trust in the Information Society 2015

[4] T. Grandison and M. Sloman. "Trust management tools for internet applications." In Proc. of the 1st International Conference on Trust Management, Crete, Greece, May 2003.

[5] M. Blaze, J. Feigenbaum, and J. Lacy. "Decentralized trust management." In Proc. of IEEE Symposium on Security and Privacy, pages 164-173, Oakland, Ca, May 1996.

[6] Quercia, D., Lad, M., Hailes, S., Capra, L. and Bhatti, S. "STRUDEL: Supporting Trust in the Dynamic Establishment of peering coaLitions." In Proceedings of the 21st ACM Symposium on Applied Computing, Dijon, France, April 2006.

[7] "Secure environments for collaboration among ubiquitous roaming entities." In Proceedings of the First Internal iTrustWorkshop on Trust Management in Dynamic Open Systems, Glasgow, Scotland, September 2002.

[8] Capra, L. "Engineering human trust in mobile system collaborations." In Proceedings of the 12th International Symposium on Foundations of Software Engineering, pages 107-116, Newport Beach, CA, USA, November 2004. ACM Press.

[9] A. Abdul-Rahman and S. Hailes. "Using recommendations for managing trust in distributed systems." In Proc. of IEEE Malaysia International Conference on Communication (MICC'97), Kuala Lumpur, Malaysia, November 1997.

[10] Ruohomaa, S., Viljanen, L., and Kutvonen, L. (2006, March). "Guarding enterprise collaborations with trust decisions - The TuBE approach. In Proceedings of the first international workshop on Interoperability Solutions to Trust, Security, Policies, and QoS for enhanced enterprise systems" (IS-TSPQ 2006). Bordeaux, France: Springer-Verlag.

[11] Marco Carbone, Mogens Nielsen, and Vladimiro Sassone. "A formal model for trust in dynamic networks." BRICS Report RS-03-4, 2003.

[12] (2017, October 24). EU Privacy law - European Union - European Commission. Retrieved from https://europa.eu/european-union/law_en

[13] The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. Retrieved from https://www.eugdpr.org/

[14] HHS Office of the Secretary, Office for Civil Rights, & OCR. (2013, July 26). Summary of the HIPAA Security Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

[15] Jesse M. Ehrenfeld, Maxime Cannesson, Monitoring Technologies in Acute Care Environments: A Comprehensive Guide to Patient Monitoring Technology (2014)

[16] J F Payne, J P Crul, Patient Monitoring (1970)

[17] MySignals - eHealth and Medical IoT Development Platform. (n.d.). Retrieved from http://www.my-signals.com/