Influencing Data Availability in IoT Enabled Cloud based e-Health in a 30 day Readmission Context

Rajesh Vargheese

Cisco, Austin, TX

Yannis Viniotis

North Carolina State University, NC

***Abstract* — The US healthcare Affordable Care Act established the 30 day readmission protection program as one of the base lines of measuring quality of care at hospitals and post discharge. With reduced payment penalties for hospitals with excessive readmissions, hospitals have increased their focus on managing post discharge care. With the emphasis on prevention and proactive care, integrated approaches that have the ability to collect relevant data from patients, process it efficiently and timely and predict risk patterns in advance and enable seamless collaboration between the patients and the care team is required. This allows care teams to proactively manage the care of the patient and limit complications and readmissions. Internet of things enabled collaborative cloud based e-health is evolving as one of the key transformation approaches in helping to address the 30 day readmission avoidance efforts. While the sensors provide critical data, there are significant constraints in terms of processing, power, storage and overall context. The power and capabilities of the cloud can augment the local visibility of sensors by providing capabilities that the sensors lack. In this work, we define these capabilities as the five P's: Provisioning, Policy Management, Processing, Protection and Prediction. We argue that by bringing these elements together, the e-health architecture is able to take the data from sensors securely and transfer it to the cloud and generate insights and actions that help improve healthcare outcomes in a timely manner. The Cloud management plays a critical role in ensuring the integrity and availability of vital information. The blind spots in the unavailability of data or compromised data can result in missed opportunities for proactive care; ours proposed architecture ensures data availability, processing availability and integrity and thus is very important in a 30 day readmission context.**

***Index Terms*—Collaboration, Cloud, Management, Internet of things, e-health, Predictive Analytics, Sensors, Policy, M2M, 30 day readmission**

I. INTRODUCTION

IN an effort to improve better quality of care, the affordable care act established the readmission protection program [1]. The program is commonly known as the 30 day readmission avoidance program and is used as a basis by the Centers for Medicare and Medicaid services (CMS) to penalize hospitals with excessive readmissions. This has resulted in hospitals wanting to proactively manage the care of patients after discharge. Based on studies by Hernandez et al., the provider engagement in the first seven days after discharge has significant correlation with chances of readmission [2]. As hospitals try to balance the resource constraints and the need to manage post discharge care, Internet of Things/Internet of Everything (IoT) enabled e-health [3] is evolving as one of the key transformation approaches in helping the 30 day readmission avoidance efforts. Obtaining vital information from patients is an important factor in enabling evidence-based medicine to prevent complications by proactively managing care. IoT enabled e-health uses sensors, machine-to-machine (M2M) communication to collect vital data from patients, performs automatic analysis by leveraging analytics and helps proactively identify trends that could result in complications and readmissions. In order to reap the benefits of such a model, an integrated architecture that brings together data, things, processes and people is required, and this architecture is the promise of Internet of Things. Studies by Dharmarajan et al [4] have shown that 13% of readmissions happen within the first 3 days, 31.7% happen within 7 days and 61% happen within 15 days of discharge, as shown in Figure 1.

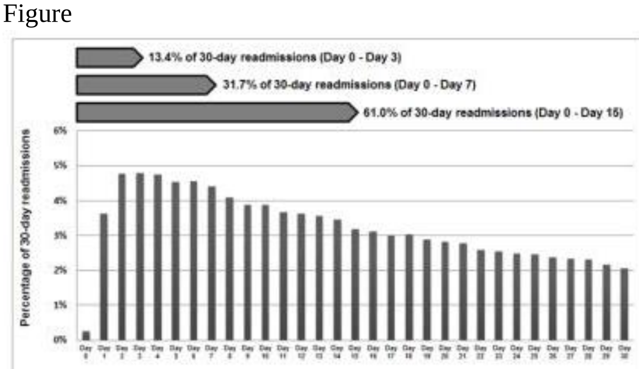

Figure 1. Percentage of 30 day readmissions reported on daily basis within first 30 days of discharge based on Dharmarajan et. al study.

Our contributions are as follows. We look at the role of cloud management of IoT enabled collaborative cloud based e-health model in ensuring information availability for proactive

July 9, 2014

Rajesh Vargheese is with Cisco, Austin, TX, USA (e-mail: rvarghee@cisco.com).

Dr. Yannis Viniotis is with Cisco and is also a professor at the Electrical and Computer Engineering department at North Carolina State University

COLLABORATECOM 2014, October 22-25, Miami, United States

DOI 10.4108/icst.collaboratecom.2014.257621

management of post discharge care. The ability of enabling seamless collaboration between patients and care teams using cloud based collaborative tools enhances the patient engagement and care outside the hospital boundaries. The management plane plays a critical role in ensuring the integrity and availability of information. We propose a cloud based e-health architecture and focuses on five management plane factors that are critical in a 30 day readmission avoidance context. We introduce the concept of blind spot in care if the management factors are ignored or missed.

The paper is organized as follows. Within Section II, we look at the current challenges in the 30 day readmission avoidance efforts. In Sections III and IV, we highlight how the proposed Healthcare IoT architecture meets the basic necessities of data availability for care. In Section V, we introduce the 5 Ps for healthcare, the cloud capabilities that play an important role in the e-health initiative in the 30 day readmission context.

II. Challenges in Enabling Proactive Care in a 30 Day Readmission Context

The 30 day readmissions problem has many challenges; in this section, we will focus on some of the aspects where e-health has a role to play. The challenges are of both clinical and technical nature. They are as follows:

A. Need for remote Vital Data collection

Evidence based clinical decisions require data from the patient. When a patient is discharged and goes out of the facility, collecting data can be a challenge because of distance, unavailability of measuring devices, connectivity, interoperability and methods of sharing data. The availability of an anywhere, anytime seamless channel between the patient and the care team can be a challenge and can take time with traditional approaches.

B. The Race against Time

The initial days after discharge are extremely critical in the readmission context. As the patient is discharged, the patient might not have any devices, and hence obtaining data might not be possible. The window of 'no data' depends on the time it takes to set up and onboard devices. The challenge is to enable data collection as soon as possible after discharge.

C. Shortage of Clinical Care Resources

The ideal post discharge scenario would be for care teams to constantly follow-up with every patient using method such as home care visits. While this is ideal, it is not a cost-effective or practical approach due to the shortage of clinical care resources that can follow up with each patient. The cost of delivering such a model is also very high.

D. Proliferation of Sensors

While the hospital might identify certain groups of patients to be at-risk and might provide them with the devices, other patients that do not fall into this category might have their own devices. As the generation of empowered patients evolves, the proliferation of sensors will continue to accelerate and hence a seamless model to collect the data from different types of sensors is required.

E. Resource Constraints in Devices

The sensors have significant constraints in terms of processing, storage and power. This prevents them from local decision processing and hence requires additional processing outside of the device that has to leverage the data from other clinical systems such as Electronic Medical Records (EMR). Similarly, with limited storage, only limited amount of data can be stored and data needs to be pushed to an external source.

F. Transforming Data to Information to Action

The sensors provide local data; however, to influence healthcare outcomes, we need insights and actions that leverage a combination of the data from the sensor and a larger context that is maintained in different systems. This requires an integrated model that ties together people, process and data.

G. Sensitivity and Threats

With the distributed nature of the patient and the provider after a discharge, the data exchange needs to be secured. The devices that are used to collect the data can be attacked and hence the challenges [5] of threats such as integrity, availability must be accounted for.

III. Internet of Things enabled Collaborative Cloud based e-Health

The Internet of Things enabled collaborative cloud based e-health brings a lot of promises in healthcare in addressing the challenges listed above. The IOT ability to create an internetworked world of data, things, processes and people enables for the first time an integrated care model to *proactively* manage care of patients effectively and efficiently. The sensors (things) collect vital information, the network transfers the information (data) to the relevant location, and the intelligence in the system (processes) identifies trends automatically without human interventions and notifies the care team (people) about the limited set of patients that they need to focus their attention on. This makes the care process very efficient and cost-effective. The clinical staff is able to make better decisions based on the data that is available from the patient's at the right time, in the right application. The ability to enable collaboration with patients anywhere using cloud based multimedia collaboration tools enable patient engagement and better care coordination. The tools can successfully enable empowerment of the patients through e-education, interaction and involvement in the patients care cycle.

The ability of auto-configuration, interoperability, self-management, intelligent interaction with other things and initiation of processes based on data and context makes the IoT enabled cloud based e-health system unique and more powerful than traditional e-health systems.

IV. ENABLING ARCHITECTURE

The primary goal of the architecture is to enable seamless collaboration between people, things, data and processes. In the e-health setting, given that the patients and care team are in different physical locations, the challenges multiply. Cloud based solutions can enable access, efficiency and provide enhanced care at a much lower cost. In this case, the architecture enables data collection and exchange, intelligent processing of the information, insight generation, data integration and access in clinical systems, and ensuring the integrity of the data both at rest and in motion. The cloud minimizes the limitations of the sensors and is the core entity that provides the majority of the functionality. The layers of the architecture include:

Sensors: Their primary role is to collect the data from the patient and hand it over to the aggregation layer. Most sensors would be wireless and in the internet of things environment, use specific protocols such as IPv6 over IEEE 802.15.4 (6LoWPAN), IPv6 Routing Protocol for low power and lossy networks (RPL) and Constrained Application Protocol (CoAP) [6] for such constraint environments.

Aggregation: The primary role is to receive the data from the sensors and transfer it to the cloud based on policies that are downloaded from the cloud. This may be a specialized device or a software mobile app running in the background.

Cloud Backend: The primary goals of this layer include, but are not limited to: enabling the communication channels, onboarding devices, defining policies and collecting the data from the sensors/aggregation layers, processing the data to identify anomalies from set targets and context, archiving the data in the clinical systems, predicting future state and generating notifications to care teams to proactively engage with the patient.

Management: The management plane of this architecture enables device discovery, provisioning and on boarding, policy management based on context and needs. The cloud based security elements monitor the traffic and protects the communication channels, data storage and applications. The management plane also enables the rapid dynamic provisioning of processing resources, and enables resource optimization.

In the current context, a hybrid cloud model is proposed to enable integration with clinical assets in the enterprise, but yet leveraging the power of the cloud to expand the reaches beyond the enterprise.

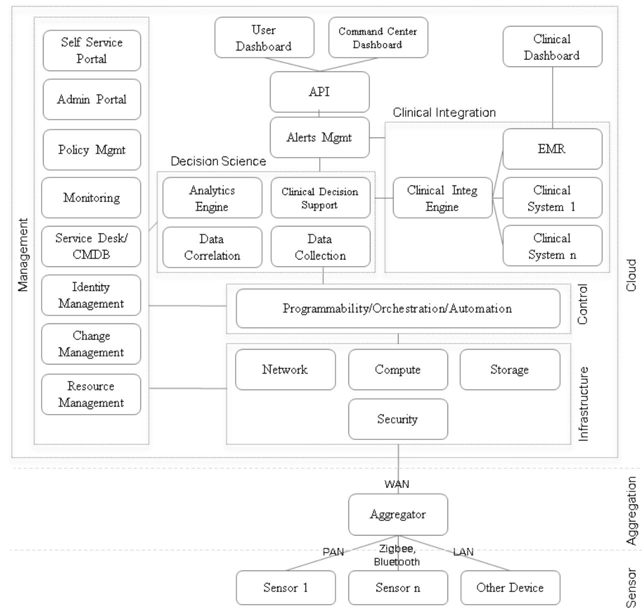

Figure 2. Architecture for IoT enabled e-health

The architecture provides integration with multiple clinical systems using integration engines and enterprise service buses. For running large scale, resource intensive tasks, the architecture uses dynamic resource allocation and scalability by leveraging Hadoop/Map Reduce technologies. The need for real time stream processing is handled by leveraging solutions such as Apache Cassandra.

V. WHY CLOUD MANAGEMENT FOR E-HEALTH: THE FIVE P'S

Innovative ideas for managing the 30 day readmission problem are evolving. IoT enabled collaborative cloud e-health is considered as an important component of such initiatives. Given the challenges we have seen in terms of the race against time, the need for quick turnarounds and seamless data exchange, Cloud management for e-health can provide effective solutions. In this section, we will look at how the capabilities of the cloud can help address some of these challenges.

To address the challenges, we will define the five P's of cloud capabilities that play an important role in the e-health initiative in the 30 day readmission context. They are defined as follows:

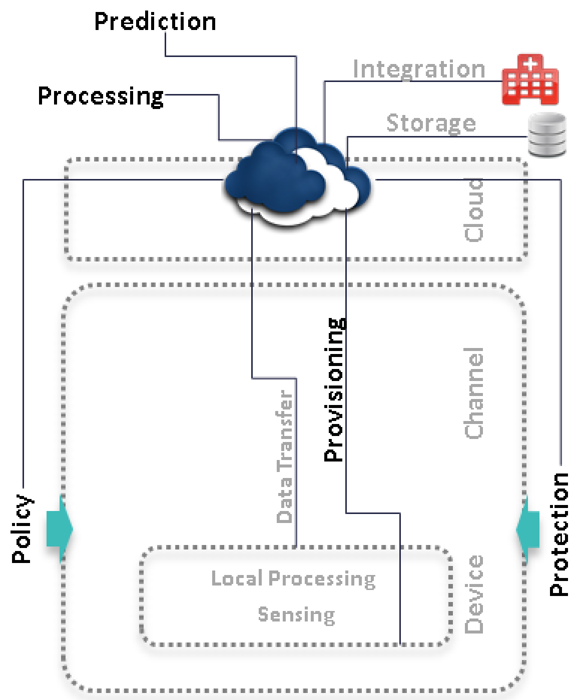

Figure 3. The five P's of cloud management that play a critical role in ensuring the data availability and integrity in a 30 day readmission context.

A. Provisioning

With the race against time, distributed nature of devices (for example a sensor inside a patient body, a sensor at a patient's home), proliferation of sensors, provisioning and onboarding plays an important role in ensuring data is available as soon as the patient is discharged. We define the time period where there is no data after a discharge as the vital information blind spot (VI_{bs}) and our goal is to reduce the blind spot.

$$T_{fda} = (1\text{-}VI_{bs}) = f\,(T_{ds}, T_{ps}, T_{ph}, T_{cs}, T_{dev}, T_{ia}) \qquad (1)$$

In equation (1), T_{fda} is the time by which first data is available after discharge, VI_{bs} is the Vital information blind spot, T_{ds} is the device setup time, T_{ps} is the provisioning time for the sensor, T_{ph} is the provisioning time for the head end, T_{cs} is the channel set up time, T_{dev} is data exchange validation time and T_{ia} is the integrated access time, which includes the time it takes to have the data processed and made available in the relevant clinical systems.

The traditional method of provisioning by sending a technician to home, setting up the device, creating the data path, configuring the sensors, calling into the hospital to configure and validate becomes unmanageable and will significantly increase the blind spot.

Cloud management on the other hand provides capabilities that address these challenges with its anywhere, anytime, any device, any channel access models, auto validation capabilities and seamless integration with other systems. Using a call home model, the sensor downloads the configuration profile and gets auto provisioned and thereby achieving an extremely small blind spot. In many cases, the need of technician to setup can be eliminated. With this model, T_{fda}, will be minimized as the dependent parameters such as T_{ps}, T_{ph}, T_{cs}, T_{dev}, T_{ia} is significantly reduced.

B. Policy Management

In a distributed architecture, with changing needs, the policies dictate the flow of information and processing. In healthcare, some policies can be dynamic and dictated by clinical decision support systems. For ex, a sensor that is capable of reporting five vital parameters might be configured by policy to send only one key metric to save resources and based on certain rules, the policy could dictate the collection of other vital signs. Such policy creation requires a global context. With the proliferation of sensors, manually configuring and changing these policies is not practical; the cloud based model can provide such a dynamic policy management and distribution capability makes the system efficient. These policies not only dictate the flow of data, they also enforce privacy and regulatory compliances such as HIPAA [7] regulations.

As needs change, policies can enable dynamic network configurations using SDN/other programmable network models. For example, if the demand increases, the traffic can be rerouted to alternate processing sites.

C. Processing

In the 30 day readmission context, alerts generated from patient vital information that are above or below the threshold are important criteria for care team interventions. Generating alerts requires not only the current data, but also enhanced processing that leverages clinical algorithms and context.

In the light of resource constraints at the sensor, it is difficult to process the data to produce alerts independently and hence the typical model is to push the event/data to an external system. Cloud can make up for the processing shortages of the sensor and can provide efficient processing leveraging the global context and massive elastic processing power.

Once the data is available, value added services such as vital sign analysis [8] and correlation solutions can be built leveraging the processing power and the platform capabilities provided by the cloud. This is important in the context of shortage of clinical resources as the automated systems are able to process the data and generate reports that provide guidance to the care teams on which patients they need to focus first.

D. Protection

While the time at which the first remote data becomes available after discharge is very important, the continuous availability of integral data is equally important. Security plays an important role in ensuring the continuous availability of data. Similar to the blind spot we defined in the provisioning section, we can define a similar model for the continuous availability of data based on confidentiality, integrity and availability. A breach of any of these distorts or distracts the care management cycle.

As the threat spectrum evolves, and with limited protection capabilities at the sensor, it is important to ensure the integrity of the data leveraging additional reinforcements outside the sensor. New innovative cloud based protection models that use behavior and learning algorithms can enable a secure e-health system. A device implanted inside the body of a patient is under heavy resource constrains to provide high degrees of encryption of data locally stored or the data that it sends from the device. This could be an attack surface if there are no additional defense mechanisms employed. In this case, cloud based security models that leverage behavior analysis, anomaly detection and deep packet inspection can become an effective cover for protecting the sensor.

E. Predictive Analytics

While it is ideal to focus on every patient that is discharged to avoid readmissions, it is neither a cost-effective nor a practical option. In such a scenario, predictive models are extremely handy to create a risk stratification model where certain patients with higher risk are managed with additional effort. Such effort includes, but is not limited to providing additional monitoring devices and constant follow-up. In many cases, such models are created based on claims and past historical data. While this is a good starting point, the 30 day readmission avoidance initiatives must also leverage dynamic data from the patient and use it to predict future possibilities and initiate an action plan to mitigate probable complications. Studies by Rothman et al. [9] have shown that incorporation of clinical variables and vital signs can be valuable to predict readmissions.

Leveraging the data received from the patient's sensors as well as data and current learnings from other data sources, it is possible to transform data into information, and then into action. However, this requires large processing, data store capabilities and wider context information. The cloud can provide such capabilities and complete the cycle from data to action and enable the full potential of e-health.

Another reason why many readmission studies have not used clinical variables is due to the challenges of data integration. The cloud management model can provide seamless integration of various clinical assets residing in disparate sources to enable a big data model from which best practices and insights can be mined. Advanced Machine learning techniques such as Random forest analysis are starting to be used in readmission prediction modeling [10] [11]. Big data solutions are also used in predicting readmissions [12].

When we look at the combined potential blind spots, there can be multiple of them, which include: (1) blind spot before the sensor is setup up and on-boarded, (2) blind spot when an attack happens and the data collection path is disturbed, (3) blind spot when data is compromised during its journey to the backend, (4) blind spot when the processing resources are not available, (5) blind spot when data reaches the backend, but does not generate the alerts due to the lack of policies and algorithms. In each of these blind spot scenarios, the cloud elements that we highlighted can positively influence the reduction of the blind spot. So, when we put these five P's of cloud management together, we assemble a very effective e-health system that can create a seamless platform that converts data to insights to action and can immensely help in the 30 day readmission avoidance efforts.

VI. CONCLUSION

The IoT enabled collaborative cloud based E-health is emerging as a key element of many 30 day readmission avoidance initiatives. The ability to collect data, process it and create targeted action plans is needed in an effective readmission avoidance plan. With time criticality and numerous challenges in existing models, the cloud management for e-health creates an efficient, secure, seamless model in provisioning, processing, protecting, enforcing policies and predicting the risk of complications. We defined these as the 5 P's of cloud management for IoT enabled e-health. By enabling such a platform, we bring together data, things, process and people to create insights and action plans early in the care cycle. This helps limit the blind spots that we described and in turn creates a proactive care model which has the potential to not only enhance the quality of life of the patients, improve operational efficiencies, reduce the cost of healthcare; but also can go a long way towards improving overall health outcomes. In summary, the cloud management of IoT enabled collaborative cloud based e-health is a critical element in ensuring the availability and integrity of vital information, which in turn is one of the baselines, to enable proactive care to avoid 30 day readmissions.

REFERENCES

[1] Centers for Medicare and Medicaid Services, "Readmission Reduction Program", Available: http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/AcuteInpatientPPS/Readmissions-Reduction-Program.html

[2] A. F. Hernandez, M. A. Greiner, G. C. Fonarow, B. G. Hammill, P. A. Heidenreich, C. W. Yancy, E. D. Peterson, and L. H. Curtis, "Relationship between early physician follow-up and 30-day readmission among medicare beneficiaries hospitalized for heart failure," JAMA: The Journal of the American Medical Association, vol. 303, no. 17, p. 17161722, 2010

[3] Lake D, Milito R, Morrow M, Vargheese R "Internet of Things: Architectural Framework for eHealth Security". Journal of ICT Standardization, River Publishing, March 2014, Vol 1 Issue 3

[4] Dharmarajan K, Hsieh AF, Lin Z, Bueno H, Ross JS, et al. (2013) Diagnoses and Timing of 30-Day Readmissions After Hospitalization for Heart Failure, Acute Myocardial Infarction, or Pneumonia Heart Failure, Acute MI, or Pneumonia Readmissions. JAMA 309: 355–363

[5] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, “Security and privacy for implantable medical devices,”IEEE Pervasive Computing, vol. 7, no. 1, pp. 30–39, Jan. 2008

[6] Bormann, C.; Castellani, AP.; Shelby, Z., "CoAP: An Application Protocol for Billions of Tiny Internet Nodes," *Internet Computing, IEEE* , vol.16, no.2, pp.62,67, March-April 2012

[7] U.S. Department of Health and Human Services, “Summary of the HIPAA Security Rule”, Available: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

[8] Alqudah, Y.A.; AlQaralleh, E.A., "A cloud based web analysis and reporting of vital signs," *Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on* , vol., no., pp.185,189, 10-12 July 2012

[9] M. Rothman, S. Rothman, and J. Beals IV, “Development and validation of a continuous measure of patient condition using the electronic medical record,” Journal of Biomedical Informatics, vol. In Press, 2013.

[10] X. Lin, A Predictive Random Forest Model on Hospital 30-Day Readmission using Electronic Health Records. MSPH, Emory University, May 2012

[11] Vedomske, M.A.; Brown, D.E.; Harrison, J.H., "Random Forests on Ubiquitous Data for Heart Failure 30-Day Readmissions Prediction," *Machine Learning and Applications (ICMLA), 2013 12th International Conference on* , vol.2, no., pp.415,421, 4-7 Dec. 2013

[12] Zolfaghar, K.; Meadem, N.; Teredesai, A; Roy, S.B.; Si-Chi Chin; Muckian, B., "Big data solutions for predicting risk-of-readmission for congestive heart failure patients," *Big Data, 2013 IEEE International Conference on* , vol., no., pp.64,71, 6-9 Oct. 2013