**Week 7: eHealth and Cloud**

Nate Bachmeier

April 21st, 2019

TIM-8101: Principals of Computer Science

Northcentral University

# eHealth and Cloud Computing

An eHealth system uses information and communication technologies (ICT), to enable both medical practitioners and their patients to gain insights into their total health. Many nations have implemented these systems with varying levels of success. This is due to their inherently complex nature as the medical facilities are politically and economically incentivized to be decentralized (Yang, et al., 2018).

## Core Subsystems

The three core subsystems to an eHealth system are (1) Electronic Medical Records (EMR); (2) Electronic Health Records (EHR); and (3) E-Prescription Services (ERX).

EMR systems address digitizing and storing medical information for regulatory compliance, sharing with authorized partner facilities, and simplifying record keeping. An EHR performs analytics, notifications, and patient dashboarding scenarios with the EMR data. ERX manages the treatment lifecycle such as refilling medications and billing insurance providers.

## Levels of Maturity

Stroetmann performed an analysis of fifty health care systems and loosely categorized them into different maturity levels. The levels are Patient Workflow Support Systems; Basic EHR-like Systems; Comprehensive, Complex Systems and Platforms; National Framework Systems with Common Components; and International Core Patient Data Exchange Services (Stroetmann, 2015).

# Reasons for Failure

## Scope Creep / Over commitment

Many eHealth systems have not acknowledged the existence of these levels and bitten off more than they can chew. Australia wasted over a billion dollars between 1999-2008 in failed systems that were meant to solve any issue that ever arose.

Then look at South Africa and Pakistan which focused on nationalized Patient Workflow Support Systems. Their solutions were narrow in scope-- handling only appointment scheduling and record storage. The patient experience was improved through reduced wait times, and the facility could focus on differentiating characteristics (Mandil, 2015) (Stroetmann, 2015).

## Too Much Tech Debt

Computer based medical records have been around since at least the 1950s, which has led to nearly 70 years of proprietary systems being deployed across the medical community. Each of these legacy systems requires a data format converter be created to connect them into modern eHealth ecosystems.

Australia disbanded their effort to catalog the requirements of these legacy systems after four years. Denmark took the opposite approach and mandated the support of open exchange protocols. They have also set a goal of only permitting four EMR systems on their national platform. For a country with 5.5 million residents this is an easier task than across the 325 million Americans or 1.32 billion Indians.

## Insufficient Maintenance

The only thing more expensive than building an eHealth system is maintaining it afterwards. Nigeria, Uganda, Libya, and other developing countries have encountered these challenges as evident by inconsistent electricity, inadequate health policies, and shortage of qualified personal (Patience & Toycan, 2016).

This has led to architectural changes such as data caching at remote branch locations which enables medical facilities to be disconnected from the network for extended periods of time.

## Cultural Barriers

Challenges caused by insufficient personal is shared by developing and wealthy nations alike. Saudi Arabia has experienced a shortage of medical professionals in part due to cultural and religious barriers.

Similarly, early attempts to bring eHealth to Ghana were also unsuccessful as they did not acknowledge these barriers. Engineering teams focused on the technical challenges of bringing Wi-Fi connectivity to remote rural communities, not devising a scheme that aligned with their religious and ethical requirements (Pagalday-Olivares, et al., 2017) (Alsulame, Khalifa, & Househ, 2015).

## Acceptance by End Users

The Taiwanese and Iraqi hospitals industry both encountered slow adoption due to the healthcare professional resistance toward the technology (Meri, et al., 2019). There was a general concern of being replaced by machines which led to avoidance of the eHealth systems. This serves as another example of the criticality of aligning personal with the technology or neither can be successful.

Australia and Malawi also experienced challenges gaining end user adoption. This was attributed to political baggage of previous failed attempts (Landis-Lewis, et al., 2015) (Stroetmann, 2015). Each platform iteration was disruptive to medical professional’s daily workflow and there was a distrust that the system would be long lasting.

System architects can address these challenges by providing clean migration paths between major releases. This adds to the cost and complexity of design but is far superior to alienating the users. Malawi was able to later gain adoption after switching to a model that sought continuous feedback from doctors and patients.

# Security, Privacy, and Liability

Few data repositories are more personal than medical records, as they hold secrets that many lacks the confidence to even tell their friends and family. Legal frameworks, such as the Health Information Portability and Accountability Act of 1996, allow patients to sue physicians and medical facilities for mishandling of these files.

## Locality

Those same requirements and liabilities extend into eHealth systems which must properly protect the data. There are additional complexities as data in the cloud might be physically stored in a region with additional requirements. Infamously, data about European citizens must reside in data centers in Europe. If the eHealth system violates this rule they can be fined for negligence.

## Identity

Several eHealth systems have avoided these challenges by operating as a gateway service and routing search requests to medical facilities which directly responsible for securing the patient information. This adds the need for federated identity as the physician needs Single Sign On (SSO) across both the gateway and the decentralized hospital network that maintains the record.

## Use of Blockchain

The use of blockchain technologies to address identity challenges is still in its infancy. Blockchain is represented as a distributed ledger where decentralized agents agree by quorum on truth values. On the surface this appears to naturally model how medical facilities are decoupled yet sharing information amongst themselves.

There are two key challenges with this approach (1) block chain protects integrity not natively support secrecy, and (2) current methods for adding secrecy involve Public Key Infrastructure (PKI) solutions (Zhang, Poslad, & Zixiang, 2018). Zhang, et. al describe this barrier to entry as too expensive for many organizations.

A disconnect in their paper is first claiming that cloud computing reduces management and operational costs of the block chain infrastructure. Yet they do not acknowledge the same to be true for PKI. Amazon Web Services (AWS) offers Certificate Authority as a Service which economically manages the problem set.

## Multi-Tenant Systems

Recently several processor defects have been disclosed which allow reading of arbitrary physical data on a machine (Horn, et al., 2018) (IEEE Spectrum, 2017). This introduces challenges for Cloud Service Providers (CSP) as they run multiple workloads on the same physical machine. If one of these tenants is malicious they can compromise the security of another tenant.

Public CSP have responded by providing dedicated physical servers to their tenants for an additional fee. While this provides assurances for Infrastructure as a Service (IaaS) scenarios it does not address more cloud native paradigms like Software as a Service (SaaS) or Function as a Service (FaaS).

Users of SaaS and FaaS gain efficiencies from transitioning infrastructure management to the CSP. Google is actively working to fill this gap with their Kubernetes platform. Kubernetes manages the lifecycle of containerized applications across a bed of machines. A container can be thought of as a micro virtual machine which is cheap to provision and destroy.

## Attack Surface

A common fallacy is that putting systems in the cloud makes them more or less secure (Teneyuca, 2011) (Gupta, Laxmi, & Sharma, 2014).