**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 have bitten off more than they can chew. Australia wasted over a billion dollars between 1999-2008 in failed systems that addressed too many problems simultaneously.

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 facility resources were free to focus on business 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 uses a different data format and must be reformatted before it can be used by modern eHealth ecosystems.

Australia disbanded their effort to catalog the requirements of these legacy systems after four years. Denmark took an alternative approach and mandated the support of open exchange protocols. They have also set a goal to reduce the number of EMR systems on their national platform to four. As a country of 5.5 million residents this they did not have nearly the scalability concerns as American at 325 million residents or India at 1.32 billion.

## Insufficient Maintenance

A comparatively expensive part to building an eHealth system is maintaining it afterwards. Nigeria, Uganda, Libya, and other developing countries have encountered these challenges as evident by their 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. Medical facilities can stay disconnected from the network for extended periods of time, and automatically resync when connectivity is restored.

## 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 the 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. Only after devising a scheme that aligned with their religious and ethical requirements did broad adoption occur (Pagalday-Olivares, et al., 2017) (Alsulame, Khalifa, & Househ, 2015).

## Acceptance by End Users

The Taiwanese and Iraqi medical hospitals industries 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 incentives with the technology or neither will 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 “this iteration of the system” would be around for long.

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 embracing and implementing 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 closest 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

HIPAA requirements extend into eHealth systems, and mandates proper data protections. 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 within Europe. If the eHealth system violates these regulations, then it will be fined for negligence.

## Identity

Several eHealth systems have avoided data sovereignty by operating as a gateway service and routing search requests to medical facilities. Those facilities are 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. The challenge is further compounded as the number of networks increases.

## 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 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 with 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 large-scale PKI systems. Having that capability negates most of their argument against using blockchain and PKI.

## 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 server. If one of those workloads is malicious, it can compromise the security of another workload.

Public CSP have responded by offering 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 argument is that putting systems in the cloud makes them less secure (Teneyuca, 2011) (Gupta, Laxmi, & Sharma, 2014). This fallacy comes from the belief that the services must be publicly exposed to be used on public CSP.

Modern cloud services can be hosted inside of Virtual Private Clouds (VPC) which limit connectivity to only VPN connections. These can be further protected through IPSec over VPN to add certificate-based protections. Partner organizations can also use VPC-to-VPC peering so that the traffic is securely routed within the CSP data center instead of using the public internet.

# References

Alsulame, K., Khalifa, M., & Househ, M. (2015). eHealth in Saudi Arabia: Current Trends, Challenges, and Recommendations. *Enabling Health Informatics Applications*, 233-236.

Gupta, G., Laxmi, P., & Sharma, S. (2014). A Survey on Cloud Security Issues and Techniques. *International Journal on Computational Science & Applications. 4. 10.5121/ijcsa.2014.4112.* .

Horn, J. H., Prescher, T., Gruss, D., Lipp, M., Mangard, S., & Schwarz, M. (2018). Meltdown: Reading Kernel Memory from User Space. *27th {USENIX} Security Symposium ({USENIX} Security 18*.

IEEE Spectrum. (2017, February 6). *Everything You Need to Know About 5G.* Retrieved from YouTube: https://www.youtube.com/watch?v=GEx\_d0SjvS0

Landis-Lewis, Z., Manjomo, R., Gadabu, O., Kam, M., Simwaka, B., Zickmund, S., . . . Jacobson, R. (2015). Barriers to using eHealth data for clinical performance feedback in Malawi: A case study. *International Journal of Medical Infomatics Volume 84*, 868-875.

Mandil, S. (2015). eHealth is health care transformation, not “an IT project”. *Eastern MediterraneanHealth Journa*, 81-82.

Meri, A., Hasan, M., Danaee, M., Jaber, M., Jarrar, M., Safei, N., . . . Al-bsheish, M. (2019). Modelling the utilization of cloud health information systems in the Iraqi public healthcare sector. *Telematics and Informatics Volume 36, March 2019, Pages 132-146*, 132-146.

Pagalday-Olivares, P., Sjoqvist, B., Adjordor-van de Beek, J., Abudey, S., Silberberg, A., & Buendia, R. (2017). Exploring the feasibility of eHealth solutions to decrease delays in maternal healthcare in remote communities of Ghana. *BMC Medical Informatics and Decision Making*.

Patience, I., & Toycan, M. (2016). A Literature Review of eHealth Sector and Challenges in Nigeria. *IEEE 978-1-5090-3784-1/16*, 145-148.

Stroetmann, K. (2015). Analysis and Typology of Global eHealth. *Global Telehealth 2015: Integrating Technology and Information for Better Healthcare*, 162-169.

Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. *Information Security Technical Report 16*, 102-107.

Yang, Y., Li, X., Qamar, N., Liu, P., Ke, W., Shen, B., & Liu, Z. (2018). Medshare: A Novel Hybrid Cloud for Medical. *IEEE Access (Digital Object Identifier 10.1109/ACCESS.2018.2865535)*, 46949-46961.

Zhang, X., Poslad, S., & Zixiang, M. (2018). Block-based Access Control for Blockchain-based Electronic Medical Records (EMRs) Query in eHealth. *IEEE 978-1-5386-4727-1/18/$31.00*.