2021

Legality and Considerations for Healthcare Chief Information Officers Migrating to the Public Cloud

Melissa Petak
Medical University of South Carolina

Legality and Considerations for Healthcare Chief Information Officers Migrating to the Public Cloud

BY

Melissa Petak

A doctoral project submitted to the faculty of the Medical University of South Carolina
in partial fulfillment of the requirements for the degree
Doctor of Health Administration
in the College of Health Professions

Legality and Considerations for Healthcare CIO's Migrating to the Public Cloud

Approved by:

Chair, Project Committee	Jillian Harvey, PhD	Date
Member, Project Committee	Mark Mellott, PhD	Date
Member, Project Committee	Larry Leaming, DHA	Date

Acknowledgements

My husband, Andrew and our children, Michael, Audrey, Luke, Sean and Christian for their patience and support.

Abstract of Dissertation Presented to the
Medical University of South Carolina
In Partial Fulfillment of the Requirements for the
Degree of Doctor of Health Administration
Legality and Considerations for Healthcare CIO's Migrating to the Public Cloud

by

Melissa Petak

Chairperson:	Jillian Harvey, PhD
Committee:	Mark Mellott, PhD
	Larry Leaming, DHA

There are many advantages for healthcare organizations to use the public cloud for storage/computing. However, moving data outside of the organization's physical boundaries implies lost or reduced control and greater reliance on Cloud Service Providers (CSP) in determining where the data is stored and how it is secured. When that data is sensitive healthcare data and at high-risk for cyber/national security violations as well as, belonging to U.S. citizens, the need for careful planning and legal compliance increases sharply. The following study evaluates the legality and considerations of public cloud use for healthcare Chief Information Officers (CIO) and the need for holistic federal regulation in order to protect healthcare data from foreign and domestic threats. Healthcare CIO's cannot continue to wait to move into the next century of technologies due to the current lack of legislative protection, which is hindering their ability to act swiftly and confidently in front of their board members, executives, peers, employees, and patients. In this study, we prove a need for the US legislative system to provide a unified legal framework that protects and enables healthcare organization to migrate their workloads/data to the public cloud using CSP's without fear of retaliation through the US legal system.

Table of Contents

CHAPTER I INTRODUCTION

1.1 Background and Need

Maintaining and staffing information technology services and hardware is expensive and unpredictable, because unexpected technical malfunctions or crashes can cost organizations millions in lost revenue. Therefore, cloud hosting companies all over the world are taking the conversation to their customers about the economics of implementing public, private, or hybrid cloud strategies and roadmaps. The public cloud is becoming an increasingly significant controversy regarding who should be regulated and how. Corporations, schools, and people of all nations have started to migrate more workloads and data to data centers owned by companies such as Google, Amazon, Microsoft, and Alibaba.

One potential reason healthcare companies are unsuccessful with developing a strategy to migrate their on-premise workloads to a public cloud hosted environment is due to cloud economics, data privacy, and cybersecurity. Comprehensive federal legislation with governing guidelines would empower healthcare organizations to move forward with this innovative solution, however, they are challenged by preemption, jurisdiction, judicial cases, private business rights, and private-right-to-action political debates. The US healthcare system has therefore, been without a safety net for the risky decision of cloud migration, and with fear of the unknown there is little movement in this direction. On the flip side, however, tech retail is leading the way to the public cloud and is experiencing massive data breeches and security issues as a result of the boom in Silicon Valley and online shopping. American healthcare leaders will not proactively adopt a cloud strategy until the US government can reassure them that they will enforce standardized regulation on their behalf. As Rubin writes in his research, there is no specific “cloud law” that guides and governs how industries interact with technologies. There is

no direct regulation for cloud services; therefore, healthcare leaders are left to navigate a matrix of different legal and regulatory rules that are as wide as the scope of technology itself (Rubin, 2019). The objective of this study is to examine federal and state court cases in order to understand policy and regulatory challenges and available solutions.

1.2 Problem Statement

On September 16, 2019, the Center for Technology Innovation at the Brookings Institute hosted a public discussion on how federal legislation should account for a variety of nuanced verticals, including health care, commerce, and education. Panelists discussed how pending legislation should allow for innovation, while still ensuring greater consumer transparency. The presenters also examined the context and application of any new law that may be created in the future and the potential effects on various online, behavioral activities managed by consumers. Privacy and security of the public cloud are the prevailing reasons why healthcare organizations are reluctant to put their data on public servers. In 2011, President Obama, through the Office of Management and Budget (OMB), established FedRAMP in order to provide joint authorizations and continuous security monitoring services for cloud services that impact all federal agencies (Health IT Legislation, 2020). The intent was for FedRAMP to help to expedite the journey into the cloud. However, in recent testimony before congress, 2019 Federal Cloud Computing Strategy, reported on some of FedRAMP's challenges and the continued need for process evolution and standardization. The United States remains at an impasse and for the past almost decade, our nation has not been able to develop a bipartisan legislation that can cut through the unsurety and duplicity of public cloud operations (To the Cloud! The Cloudy Role of FedRAMP in IT Modernization, 2019). CloudSmart has reported on some of FedRAMP's challenges and the continued need for process evolution and standardization. CloudSmart stated that "a lack of

reciprocity across agencies when adopting FedRAMP authorizations has led to significant duplication of effort when assessing security for product deployment." Ultimately, making it too complicated for agencies to issue an Authorization to Operate (ATO) for solutions/projects that are a good public cloud fit.

Microsoft, a hard charger in this space leading with their cloud product, Azure, is forcing their customers to migrate to cloud hosted Office 365 and Windows 10 or pay support costs per user license to remain on the old technology. The Pentagon awarded the largest cloud computing project business to Microsoft in October 2019 causing an outbreak of cloud first strategies within healthcare fast follower companies. After the US government awarded Microsoft the contract, Amazon sued the government basing it on interference from President Trump. This is one more reason why Congress is being forced to step in and develop regulation around public cloud usage and protection (The Guardian, 2020). Without the right laws/regulations that protect cloud providers, healthcare companies and patients the judicial system will likely be overwhelmed with legal cases like this.

Additionally, after the healthcare giant, Ascension signed an agreement with Google to host their patient's medical data in Google's public cloud; several lawsuits and congressional hearings arose. Shortly thereafter, a lawsuit was filed by a patient against Sutter Health System out of Sacramento, California regarding Sutter Health System because they were found sharing patient data with Facebook and Google. The lawsuit alleges that Sutter Health patients are most likely unaware that their information, including search history on subjects like cancer and sexually transmitted diseases, is being shared with third parties. Also, patients in the lawsuit accused Sutter Health of seven causes of action, some of which are violation of California's Invasion of Privacy Act and the Confidentiality of Medical Information Act. The data disclosed

by the defendant to Facebook, Google, and others in this case is 'medical information' under the Confidentiality of Medical Information Act (CMIA) because it includes information derived from the defendant regarding its patients' medical history, physical condition, or treatment (Drees, 2019). It's only a matter of time before more lawsuits are filed, which could build fear within the healthcare industry to partner with public cloud providers and force the US court system to set the strategic path forward. Per Ascension's Congressional hearings, there have been multiple incidents that cause serious concerns about Google's (Alphabet, Inc.) ability to safeguard sensitive health and medical information properly. "Personally identifiable healthcare data was being haphazardly transferred to Google without proper safeguards and security in place" (Landi, 2019). Unless the proper safeguards and security are defined, it is a moot point to continue to point out the violations.

1.3 Definitions

Cyber Security - Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security (Kissel, 2019)

Application - A software program hosted by an information system (Kissel, 2019).

Data Security - Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure (Kissel, 2019).

Data Privacy - Restricting access to subscriber or Relying Party information in accordance with federal law and agency policy (Kissel, 2019).

Public Cloud - Public cloud solutions are readily available from Google, Amazon, Microsoft, and others. Public cloud services provide infrastructure and services to the public, and you, or

your organization, secure a piece of that infrastructure and network. Resources are shared by hundreds or thousands of people (Technology Services, 2020).

Private Cloud - Private cloud solutions are dedicated to one organization or business and often have much more specific security controls than a public cloud. Private cloud solutions utilize infrastructure that is either owned and controlled by the organization, or they are able to contractually require those specific criteria be met by a vendor who manages the infrastructure (Technology Services, 2020).

Hybrid Cloud - Hybrid cloud solutions are a blend of public and private clouds (Technology Services, 2020).

Encryption - Conversion of plaintext to ciphertext through the use of a cryptographic algorithm (Kissel, 2019).

Cloud Computing - A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud). Note: Both the user's data and essential security services may reside in and be managed within the network cloud (Kissel, 2019).

Data Workloads - In computing, a workload, typically, is any program or application that runs on any computer. A workload can be a simple alarm clock or contact app running on a smartphone, or a complex enterprise application hosted on one or more servers with thousands of client (user) systems connected and interacting with the application servers across a vast network. Today, the terms *workload*, *application*, *software,* and *program* are used interchangeably (What is hybrid cloud? Everything you need to know, 2020).

1.4 Research Questions

Are U.S. healthcare laws and regulations that exist today sufficient to protect healthcare data stored in the public cloud, and if not which gaps remain? The author's hypothesis is that there is insufficient regulatory protection over the use of the public cloud for use in the healthcare industry, i.e., patient data, genomics, electronic medical records, research compute, and clinical workloads. Without regulations from the United States legislative branch, healthcare data and corporations are at risk of a serious threat to our national security. Countries in Europe and India have recently made serious regulatory changes in order to protect healthcare data by passing such laws as the DISHA (India, 2018) and the General Data Protection Regulation (European Union, 2018).

The following questions are the focus for this study:

(1) What are the current regulations and laws pertaining to healthcare and the use of the public cloud?

(2) What are the current court cases (both state and federal) that pertain to public cloud providers regarding healthcare data/privacy/use?

(3) What are the gaps in the requirements that need to be met for hospital CIO's to move their data and workloads into the public cloud safely?

2 CHAPTER II SCOPING LITERATURE REVIEW

2.1 Literature Review Methods

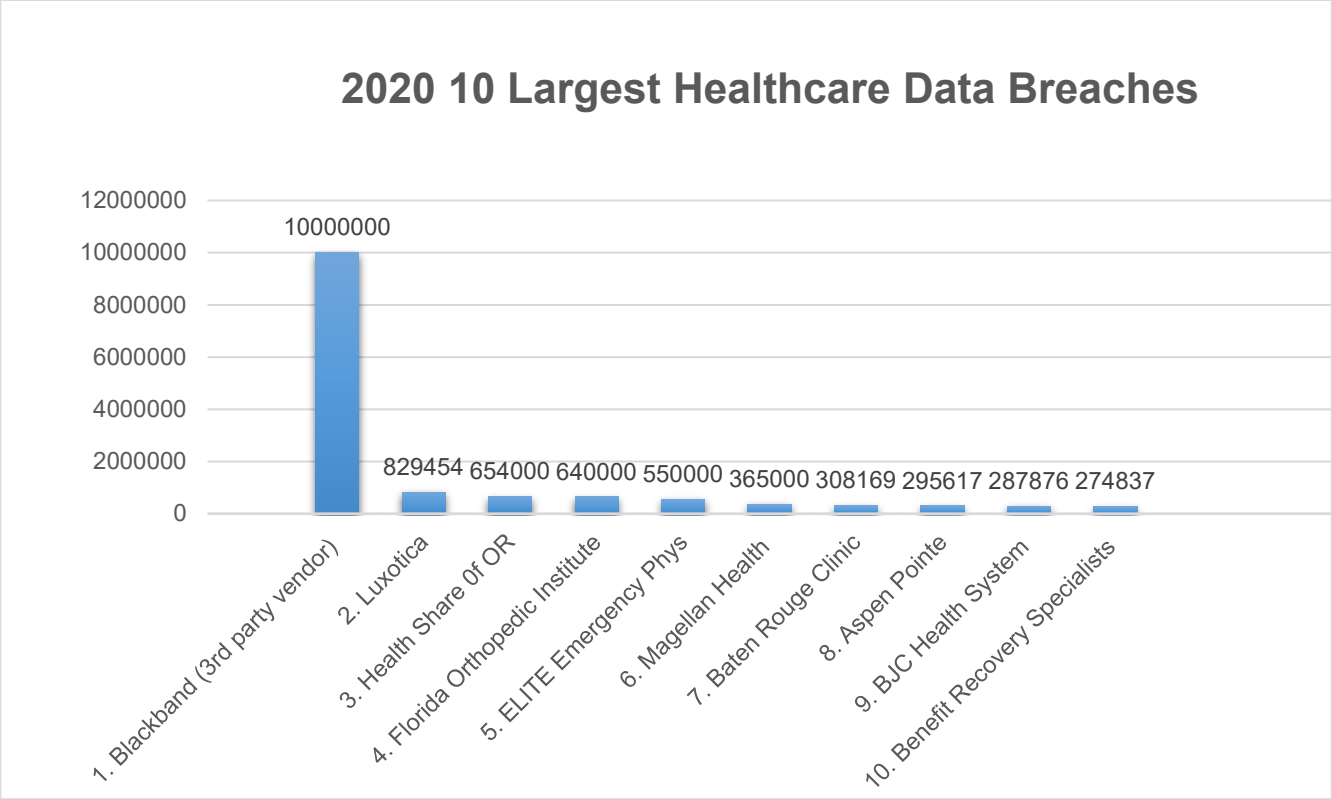
Using PubMed.gov the following terms were searched, “public cloud” and “healthcare” resulting in 52 articles from 2002 to 2020. Of the articles that were found, only 22 articles contained information that outlined security/regulatory concerns with healthcare use of the public cloud for data storage/computation. Common themes found throughout the 22 articles reviewed include data security, data privacy, cybersecurity, security safeguards, encryption, and device security. However, an overarching gap is the absence of legislative protection for national security related sensitivities such as healthcare data in the public cloud. Similar to our country’s need to secure its borders from invasions, and hostile threats, the cyber borders of our country should be protected much the same way. The legislative branch has the responsibility to establish regulations that protect the American consumer from known and unknown threats, as well as protect healthcare organizations storing sensitive healthcare data and workloads with public cloud companies.

2.2 Security and Privacy Themes

Electronic Personal Health Information (ePHI) is protected under HIPAA laws and its successors (i.e, HIPAA Final Security Rule/HITECH/GINA/Omnibus) which indicate that ePHI must be encrypted and de-identified for sharing or storing in the public cloud. HIPAA laws established three categories of safeguards: administrative, technical and physical. However, no enforcement exists to ensure that technology companies adhere to these requirements, which places the burden of proof and compliance on healthcare organizations to comply with federal law when using such technology vendors. Researchers have demonstrated that data breaches still occur today due to inadequate device security, not following administrative safeguards,

unsecured hardware, unsecured network cables, non-compliance with physical safeguards, lack of adequate fire protections, non-compliant software vendors, lack of audit trails, no use of unique user logins and passwords, and no encryption at rest (Mohammed Naveed, 2018). These concerns can be easily addressed using the healthcare public cloud – but how does a CIO ensure that the public cloud vendor is adhering to the measures that have been outlined by the HIPAA laws?

Figure 1: Data Breaches



Recently, due to the COVID19 pandemic, the US government has responded to the need for more healthcare data transparency and accessibility for its citizens by passing the Cures Act in March of 2020. "The days of patients being kept in the dark are over," said CMS Administrator Seema Verma upon passage of the Act.

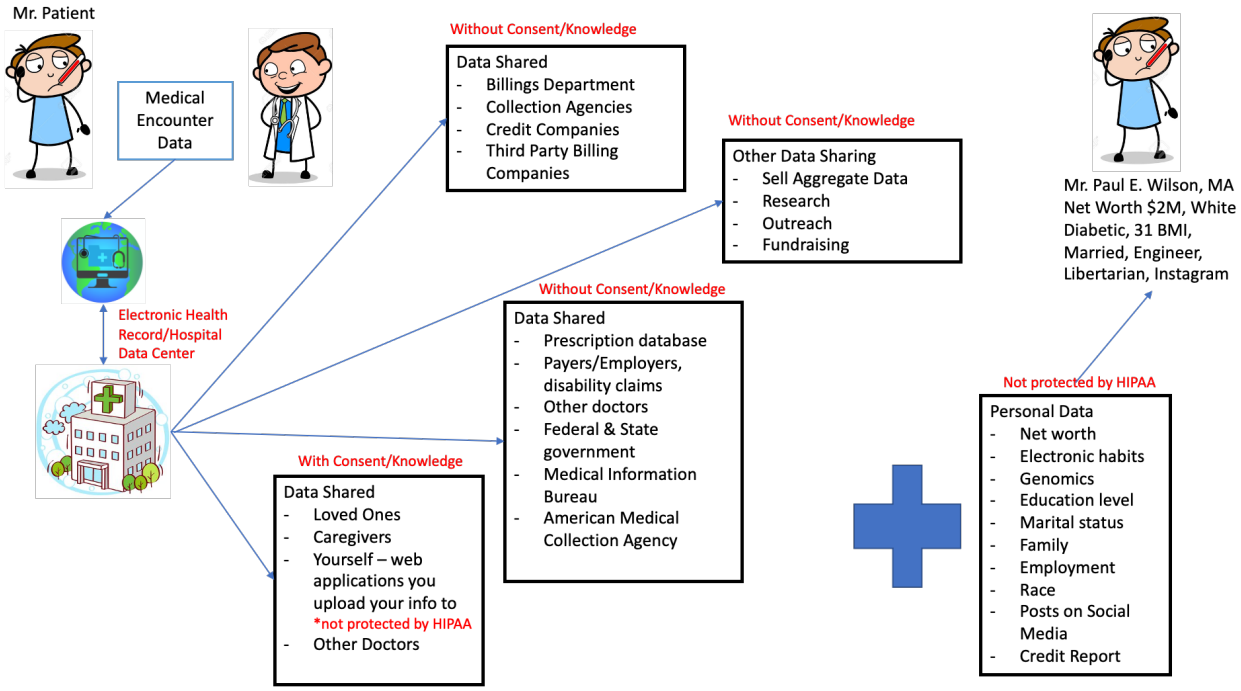
> In today's digital age, our health system's data sharing capacity shouldn't be mired in the stone age. Unfortunately, data silos continue to fragment care, burden patients, and providers, and drive up costs through repeat tests… these rules begin a new chapter by requiring insurance plans to share health data with their patients in a format suitable for their phones or other device of their choice. We are holding payers to a higher standard while protecting patient privacy through secure access to their health information. (Centers for Medicare and Medicaid, 2020, para. 6)

However, this congressional response is not addressing the need for audit trails, device security, cybersecurity, and encryption across all public clouds/non-mobile devices.

A lack of regulation that secures the sovereignty of our borders regarding healthcare data in the public cloud is a national security risk, and our nation's legislative branch needs to take action immediately. As stated in numerous research articles, there is a gap in US policy around healthcare data protection in the public cloud. The average US citizen has no knowledge where their healthcare data is being stored in the continental USA or overseas in another country's database; making the data invisible to the end user doesn't meet the requirement for consumer transparency. When patients share their medical and personal data with a provider or hospital system, they assume that their information will be safeguarded. Current research does not demonstrate that the healthcare industry sufficiently understands the interoperability and life cycle of healthcare information. Encryption and de-identification are a start, but genomics research has demonstrated that it is not enough. According to Naveed (2018), "A more recent study showed that genomic data could be reidentified to the individual using a combination of the genomic data and phenotypic traits gathered from public databases, photos, and social media" (Mohammed Naveed, 2018). American policymakers could do more to protect people's

information. In the United States, companies can harvest personal data unless a specific law bans it, thus California just passed legislation that could create restrictions, said William McGeveran, a professor at the University of Minnesota Law School. Europe, in contrast, passed a strict law called the General Data Protection Regulation, which went into effect in May. "In Europe, data protection is a constitutional right," McGeveran said (Allen, 2018).

Figure 2: Example of Healthcare Data Protected and Not Protected by HIPAA



2.3 Healthcare Data Protection Laws and Threats

A handful of research articles mention a lack of regulated data protection/security with regard to the use of public cloud for genomics data while at the same time, contrary to these security concerns, researchers advocate the benefits of public cloud technologies for the advancement, cost-savings, research, flexibility, adaptability, and scalability of the healthcare industry (Gavriloc & Trajkovik, 2012). Most research focuses on the ground breaking

advancements that occur with artificial intelligence, machine learning, high-capacity computing, complex algorithms, and hardware/staff cost savings. While research scientists are hyper-focused on the biosciences, and possibilities of combining computer engineering with biology – the researchers fail to highlight the risk of data protection/security that CISO's and CIO's are facing every day. Research articles that look at hospital/healthcare systems use of the public cloud for their operational data, medical/clinical data and administrative data were not found. Hospital IT staff are charged with the responsibility of providing a secure infrastructure for consumption by clinical, administration, and operational departments. This does not mean that these departments do not procure/purchase online resources such as, Amazon Web Services, etc. without the knowledge of the hospital IT staff in order to bypass the long wait times, or backlog of internal infrastructure requests. Research does not address administrative/policy gaps within and outside of healthcare organizations.

There is a strong need for the US government to establish healthcare-centric laws that protect patient/medical data from exposure through migrating their data to public cloud providers. The public cloud offers new possibilities for healthcare organizations, such as big data analytics, ubiquitous access to EHRs, blockchain, biogenetic computing, cost savings and scalability. Security and privacy are a major factor in the cloud computing environment, as well as lack of a standardized Business Associate Agreement (BAA) for public cloud partnership, and the shortcomings of U.S. federal policy to safeguard the healthcare data owner faced with a biomedical or bioenvironmental data exposure (Harshbarger, 2011).

As Majumber has argued, the United States (US) lacks a "comprehensive data protection regime." One data protection law tends to contradict the other. Data protections are disjointed,

> "spread across bodies of law that target specific kinds of research or data generated or held by specific kinds of actors involved in the delivery of health care. Oversight is also distributed across a range of bodies, including institutional review boards and data access committees." (Majumder, 2018)

As the sophistication of attacks against data centers and businesses grows, the need for additional, highly trained cyber security experts and sophisticated hardware additions must be implemented. At any level, these resources are going to be required, regardless of the size of an IT department.

The New York Times reported that the Trump administration was considering limiting the access of Chinese researchers to US technologies, based on national security and economic competitiveness concerns (Majumder, 2018). China is not only a threat to our healthcare data security, they are already gaining access to American health and genomic data through the US health care system. "Chinese companies have access to American health and genomic data including through accredited corporate participation in the US health care system… China's efforts to acquire US health data combined with limited protections raise questions about national security" (Davis, 2019). The US government needs to develop federal guidance for international data agreements to protect access to aggregated data on US citizens. The policies would outline how to structure those partnerships so US interests are maintained. With greater policy intervention from the national government, healthcare corporate leadership would have the processes and standards that they needed to protect patient data. Eddy points out that cloud-based data breaches were one of the "three major information security threats that healthcare organizations will have to watch out for in 2019 and years that follow" (Eddy, 2019).

Additionally, "… also stressed (was) the need for greater cybersecurity to protect the data of US patients" (Davis, 2019).

A 2019 report from the US-China Economic and Security Review Commission established by Congress stated that, "The U.S. doesn't protect medical and healthcare data as well as other nations. Citing the strict nature of EU's General Data Protection regulation, HIPAA and other US regulations do not go as far to protect patient health data" (Davis, 2019). Some recent policy changes have addressed protection of future open cloud-based healthcare data and some laws and regulations were changed to directly support new kinds of cloud initiatives (Kleyman, 2018). For example, the HIPAA Omnibus rule enacted in 2013 now allows third parties to become business associates (BAs). A BA is any organization that has more than just transient access to data (e.g., FedEx, UPS, USPS). An organization can sign the Business Associate Agreement (BAA) and assume additional liability to manage Protected Healthcare Information (PHI) (Kleyman, 2018). Should companies wish to develop products for medication delivery or secure file transfer, outside of their normal lines of business, they can enter into a BAA to assume liability for safeguarding the data they access. Importantly, the mindset is shifting as it pertains to pushing more data toward the cloud. "By 2021, researchers predict public cloud service providers will process more than 35 percent of the healthcare industry's IT workloads" (Kleyman, 2018).

2.4 Research Gaps

These are great strides forward but policy makers aren't doing enough. Current legislation only addresses the minimum standards of PHI security and privacy. The healthcare industry's best practices advise for additional and more rigorous measures to protect patient/medical data. In 2015, over 120 million health records were breached, which is cause for

this growing concern (Clear Data, 2019). Additional policy to help interrupt and deter malicious attempts to gain access into medical records and company data are critical to the success of healthcare cloud benefits. Although there is often a reference to HIPAA as being the overarching protection for all healthcare data, regulations issued by the HHS Office for Civil Rights (OCR) under HIPAA apply only to "covered entities" and, to a more limited extent, their "business associates" (Clear Data, 2019). This means protections do not attach to all personal health related information created or circulating within the US; rather protection depends on the status of the "data holder" (Kavita M. Berger, 2019). Berger's study was limited to researchers sharing genomic healthcare across hyperspace and missed out greatly on the risks beyond HIPAA. Using a public cloud service extends the trust boundary beyond the organization. New risks are introduced by utilizing CSPs (Cloud Service Provider), such as insider threats and a lack of control over security operations. A main difficulty of moving into the realm of cloud computing is having to rely on the CSP vendors to provide adequate documentation of their policies and procedures along with the ability to audit, physically or digitally, access to any data contained on their servers.

2.5 Legal Review

There are several legislation actions worth discussing in this report, the HIPAA laws and regulations, the Clarifying Lawful Overseas Use of Data (CLOUD) Act, and the Affordable Care Act – HITECH Act. Two key elements of the CLOUD Act are the provisions for U.S. access to foreign stored data and the provisions to create executive agreements for foreign access to U.S. stored data. The CLOUD Act is legislation that developed in response to the Supreme Court case of the US vs. Microsoft, which occurred because the US government had access to data stored by Microsoft in their data centers in Ireland. Prior to the CLOUD Act, US agencies,

private businesses, and US citizens did not have any rights that protected their privacy or access to data stored overseas. This is also a major concern for healthcare leadership when they are considering potential public cloud vendors. Healthcare companies and their leadership have a responsibility to the public they serve to safeguard medical/healthcare data as well as, personally identifiable information. However, the CLOUD Act does not extend standards for cloud hosting vendors to protect American businesses who have made contractual agreements to store and process data outside of their own managed and run data centers. Protection for the healthcare industry lies in their legal departments' abilities to implicate the cloud provider as the accountable party to any data breeches or cybersecurity hacking. Due to the legal inconsistencies, these agreements rarely get out of the legal department of hospital organizations, healthcare payer systems, and providers office. Ultimately, this dilemma slows and diminishes the technical advantages and compute analytics of cloud usage for the healthcare industry pushing it further and further behind other public service industries staying current with technological trends and norms. For example, the recent COVID19 pandemic revealed that most hospital systems were not postured to enable their workforce and treatment facilities to scale in a virtual environment for telework; most rural hospitals did not have enough devices (phones, laptops, and tablets) to issue their employees and send workers home for business continuity. In order to adapt to offering services remotely, Cayuga Community Health Network in rural Cayuga County, New York, upgraded all its computers and adapted all its community programs so they can be offered via Zoom and Facebook Live. The network uses its website and Facebook page to provide weekly health tips and share information with community partners (Weiss, 2020).

Health Insurance Portability and Accountability Act (HIPAA) laws and regulations have also been key to how healthcare systems procure technical/data services. Often, we hear that a tool is HIPAA compliant, or HIPAA certified but most of the time, that doesn't mean the same thing to everyone. There are two main aspects of HIPAA: privacy and security. HIPAA privacy is further along than data security with public cloud vendors and the industry making significant advances in the fields of data encryption and deidentification of patient data. HIPAA has established national standards to protect individuals' medical records and other personal health information and applies those standards to health plans, health care clearinghouses, and health care providers who conduct certain healthcare transactions electronically. (O'Dowd, 2020) However, this legislation was created decades ago and is not current to meet today's needs/demands in the growing technology hyperspace.

Table 1: United States Federal Laws and Security Regulations pertain to Heathcare Data

Regulation	***Date Enacted***
FERPA	*January 8, 2009*
HIPAA Privacy Rule	*April 14, 2003*
HIPAA Final Security Rule	*April 20, 2005*
HITECH	*February 17, 2009*
Cloud First Act	*Februry 8, 2011*
GINA	*May 21, 2009*
Cloud Smart Act	*October 2018*
FEDRAMP	*June 2012*
FISMA – Information Security Act	*2002 (updated 2014)*
CLOUD Act	*March 23, 2018*

HIPAA Omnibus Rule	*September 25, 2013*
Cures Act	*March 2020*
MACRA (shift to equality of care model)	*April 16, 2015*
The Confidentiality Of Medical Information Act (CMIA)	*August 22, 2013*
HR 5901 – Information Technology Modernization Centers of Excellence Program Act	*December 3, 2020*

Regarding security, the HIPAA Omnibus Rule is potentially the biggest factor facing healthcare public cloud roadmaps today. The Omnibus Rule states, "make entities that are defined as business associates (BAs) directly accountable if they run afoul of the regulations." In the area of data breaches [before the Omnibus Rule], BAs only needed to notify covered entities in breach cases that could result in significant risk of financial/reputational harm. But under the Omnibus Rule, any disclosure of patient data is subject to notification (unless the BA can demonstrate a low probability that the PHI has been compromised) (O'Dowd, 2020). The Omnibus Rule is ultimately putting the liability for compromises on the healthcare entity unless they can prove that the Business Associate (cloud hosting vendor) is directly accountable. Hence, the delay in legal agreements and complicated data sharing rulesets. While BAs [Business Associates] are directly liable under HIPAA, covered entities are also directly held responsible for any actions of their BAs. This fact alone argues for following a rigorous process when selecting your cloud-based service providers (Arango, 2019). Putting the legal battle and nightmare of accountability and finger pointing aside, the cybersecurity landscape is growing and changing on a daily basis and at record pace. While the world is moving to scalability and flexibility which can only occur through cloud hosted solutions, there is still the need for

stronger and more robust micro-segmentation, network duplication, decoy IP addresses, and strong offensive cyber counter-attacks. These topics are blind spots to most, if not all, healthcare CEO and CMOs. Healthcare leaders are faced with a dual mission that they were not educated or trained to execute: delivering healthcare benefits and protecting them from cyber-attacks.

The Affordable Care Act (ACA)/HITECH Act, signed into law in 2009 by President Obama, enhanced the previous HIPAA laws in order to provide for Healthcare Exchange Reference Architecture, Electronic Health Record (EHR) adoption, and Federal Data Sharing guidelines. The HITECH Act, which is a part of the ACA, established the guidelines for clinical data sharing through the implementation of electronic medical records and interoperability across previously segmented systems. The HITECH Act was the first step in government legislation pushing the healthcare industry toward technology adoption/advancement. As one researcher stated,

> The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, provides [Agencies] with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange (Arango, 2019; Health IT Legislation, 2020).

Moving patient's medical and health data to an electronic format with a unified healthcare data reporting standard led to improved analytics reporting which impacted patient outcomes significantly. The HITECH Act, was a precursor to the public cloud journey for many healthcare companies; the sheer amount of data now being collected from EMR's and EHR's, cannot be analyzed without high-power computing which are mostly available in the public cloud. Hence, the need for public cloud legislation for healthcare companies that cannot

adequately take advantage of their data, until they are able to safely and confidently eliminate the risk of not having physical custody of their data/information.

2.6 Gaps in Laws/Regulation

Congress has been struggling to regulate the internet and public cloud since, it was unveiled back in the 1980s; in the absence of regulation, it is the wild west for computer programmers. According to the National Bar Association Website,

> ...cloud-based data that [does] not involve electronic communications are not protected… for example, if you upload personal financial data to iCloud or Google, your financial information would not be protected by SCA because there is no communication involved. But, if your gmail account is backed up to google drive, you are protected by SCA. (Arango, 2019).

Thus, most cloud data are unprotected by the SCA. Given Congress' lack of deliberate, bipartisan direction and leadership regarding public cloud legislation drafted to protect healthcare privacy and security, legislators are unintentionally shifting this issue to a settlement within the judicial system; it is being hashed out in court cases around the world. Instead, Congress needs to address cloud privacy with legislation. Erin Murphy,

> Cloud storage is a highly complicated area that requires a depth of fact-finding and deliberating not suited for the judicial system. Of course, Congress has not always been reliable at legislating technological issues, but Congress's struggles should not provoke a judicial response (Murphy, 2013).

Additionally, Congress is struggling with the role of the states versus the federal government with regard to public cloud regulations. There are court cases today, as mentioned in the Brookings panel interview, within the state of California concerning data privacy, as well as, Ascension and Sutter Health Systems. If Congress steps in and makes laws that override state laws, it is called preemption. Preemption is a big factor, according to Brookings that is delaying a unified federal public cloud regulation for industries demanding it – one of which is healthcare.

Lastly, the final issue that is delaying a congressional law to protect Americans against public cloud threats is free market rules that we as a capitalistic nation have silently agreed to. This means that businesses are left to decide how they deem most appropriate to conduct business without the threat of government micro-management. Government should be available for oversight and citizen protection, but they can't intervene and tell a vendor how to run their business. So far, the government has been very prescriptive with Cloud First and Cloud Smart strategies for their own agencies and operations however, they are not interfering with private industry and their cloud vendor contracts unless a legal case makes its way up to the Supreme Court. Correspondingly, we are seeing start to this exact scenario happen as a result. The public is unaware of most malice and threats on the public cloud due to the hidden and dark nature of the internet, but it is the US government's responsibility to protect their citizens against all threats foreign and domestic. This issue is creating a dichotomy of inconsistency between private business and public cloud for healthcare specifically meaning that if a healthcare company decides to host their EMR in a public cloud and there is a security compromise, is the cloud provider liable because they had a responsibility to deliver a certain product to the healthcare company? Or is the healthcare company liable because they are accountable to

HIPAA and HITECH rules? These questions need to be answered by congress in order to stop slowing down the advancement of public cloud technologies across the healthcare industry.

3 CHAPTER III METHODOLOGY

The goal of this study is to develop a CIO Public Cloud Checklist and assessment tool for public cloud providers, as well as, a comprehensive review of court cases involving healthcare public cloud search parameters and current laws/regulations.

Thus, our review questions are:

(4) What are the current regulations and laws pertaining to healthcare and the use of the public cloud?

(5) What are the current court cases (both state and federal) that pertain to public cloud providers and healthcare data/privacy/use?

(6) What are the gaps in the requirements that need to be met for hospital CIO's to move their data/workloads into the public cloud safely?

In this study, we will examine the need for the US legislative system to provide a unified legal framework that protects and enables healthcare organization to migrate their workloads and data to the public cloud using CSP's without fear of retaliation through the US legal system. This study will provide a checklist that enables CIO's to ensure that their data center environments are cloud ready, and that all security best practices are met. This study will also review current and past legal cases pertaining to CSP's and healthcare organizations in order to present CIO's and healthcare leadership with a list of risks when using CSP's.

Carrying out the review comprised the four stages of (1) collecting legal cases through a HeinOnline.org database search, (2) a first relevance screening to filter the results, (3) a review of the legal cases and (4) a summarization of the content based on the court/judge decision/outcomes. In this review, the concept of healthcare includes all activities related to diagnosis, therapy, and prevention of human diseases or injuries, as well as clinical research, healthcare management, and use of the public cloud for data sharing when a healthcare entity has an agreement to put their production/non-production workloads into the data centers/servers of a public cloud provider.

3.1 Search Strategy

This study will review all laws that pertain to the use of the public cloud, and healthcare data security and privacy. The laws will be reviewed in order to create a matrix of rules/standards that will either enable or preclude the use of the public cloud for hospital CIO's.

Study Objective	Research Methods and Data
What are the current regulations and laws pertaining to healthcare and the use of the public cloud?	HIPAA, HiTrust and applicable guidelines/laws/regulations review
What are the current court cases (both state and federal) that pertain to public cloud providers and healthcare data/privacy/use?	Federal and state court cases by searching LexisNexis, literature review
What are the requirements that need to be met for hospital CIO's to move their data/workloads into the public cloud safely?	Interviews with CIOs, Europeon laws/regulations for public cloud usage

HeinOnline.org case law database was utilized with the search phases "healthcare" and "public cloud" in 2016 – 2021. Results were as follows: (27) Law Journal Articles, (15) U.S. Congressional Documents, (5) U.S. Federal Agency Documents, Decisions and Appeals, and (2) Cases. Search results when using the terms "medical data" and "public cloud resulted in (13)

Law Journal Articles, (1) Case, (1) Reports of U.S. Presidential Commissions, (4) U.S. Congressional Documents, and (1) U.S. Federal Agency Document, Decision and Appeal. Further, articles were subsequently included based on references in the publications of this first search. All cases and articles were further reviewed to include the following information in order to be included in this study:

- HIPAA, HITECH, FedRAMP, Cloud Law, or BAA
- Public Cloud Provider – Amazon, Microsoft, Alibaba, Google, IBM, or Oracle

All references were imported into the literature management program – OneNote. All results were screened for relevance against our inclusion criteria (stated above). Additionally, google searches were conducted with the words "healthcare lawsuits against public cloud" which resulted in the top eight cases that were reviewed.

3.2 Selection of Studies

The review team consisted of one researcher with expertise in healthcare, computer science, medical informatics, and statistics. Cases were read and reviewed and scored with the appropriate indicators per the scoring terms established by the review team mentioned below. Due to the rate of advancement of technology, all legal cases and law reviews that were older than January 2018 were excluded. Only cases from January 2018 to March 2021 were reviewed. Only legal cases were reviewed and all other articles were removed, as well as any erroneous results that showed up in the filter based on name associations with "public cloud" or "healthcare."

Additionally, the remaining legal cases were scored with a value based on the presence of healthcare applicable privacy and security laws, and then if a public cloud provider (Microsoft, Amazon Web Services, and Google) were included. Cases without these two distinct criteria were excluded. The highest eight legal cases were distinctly scored with a yes or no, based on two criteria above in order to be included in the study.

3.3 Outputs

The results from the legal case reviews will be analyzed for any lessons learned or relevant information that would help to guide the CIO cloud checklist. Legal case reviews will look for outcomes related to cyber insurance, liability rulings, terms of service, data privacy and security, punitive outcomes, and breach of contracts. Additionally, the final results of both the legal case review and expert interviews were used to develop the checklist for CIO's to use when considering migrating their on-prem workloads to the public cloud.

3.4 Research Design or Method

The research is a qualitative study that consists of a legal case study, and expert interviews with four Hospital System Chief Information Officers regarding their thoughts and impressions of healthcare data/workloads running in the public cloud.

3.5 Instrumentation and Data Collection

One set of interview questions was designed and used to interview a minimum of four hospital/healthcare CIO's. Knowing that not all CIO's would be responsive or available to respond, the investigator invited 10 hospital CIO's to participate. The hospital CIO's were selected using a convenience sample, to provide a mix of size of hospital systems, diversity of patient population, hospital type, and geographic location. Altogether two childrens hospitals, three university hospital systems, four for profit hospital systems participated in the interviews.

Five open-ended interview questions that were all designed to be open-ended in order to allow the executives to elaborate where they desired. Questions were validated through feedback from field experts in healthcare IT and modified to fit the objectives of the study. The interview questions were then emailed to the CIO's in addition to a short description of the research project asking for the CIO's participation prior to the interview. The CIO was given the option to schedule a 30 minute Zoom recorded call with the interviewer. The same investigator conducted all interviews in order to provide a consistent experience.

The questions are as follows:

1. What requirements need to be met for your organization to safely and confidently move healthcare data/workloads to the public cloud?
2. Which of the requirements that you have listed from above do you feel you cannot meet today? And which ones do you believe have been met?
3. How would federal legislation aid your organization in safely/securely moving data/workloads to the public cloud?
4. Do you believe that the other countries policies (EU/India) as it pertains to securing the use of the public cloud for patient/citizen data are further along than US policy? If so, how so?
5. What is your greatest fear or hesitation in moving healthcare data/workloads to the public cloud?

3.6 Data Analysis

An inductive thematic analysis of the qualitative data will guide the development of a CIO Cloud Checklist. A preliminary coding structure will be inductively developed based on the recommendations from the literature and legistlation. Key informant interview transcripts will

be systematically read to identify emerging categories and to identify gaps that are not captured in the literature (Brooks J, 2015). Codes will be grouped to form themes that will guide the creation of the checklist items.

4 CHAPTER IV JOURNAL MANUSCRIPT

4.1 Background

Maintaining and staffing information technology services and hardware is expensive and unpredictable, becuase unexpected technical malfunctions or crashes can cost organizations millions in lost revenue. Therefore, cloud hosting companies all over the world are taking the conversation to their customers about the economics of implementing public, private, or hybrid cloud strategies and roadmaps. The public cloud is becoming an increasingly significant controversy regarding who should be regulated and how. Corporations, schools, and people of all nations have started to migrate more workloads and data to data centers owned by companies such as Google, Amazon, Microsoft, and Alibaba.

One potential reason healthcare companies are unsuccessful with developing a strategy to migrate their on-premise workloads to a public cloud hosted environment is due to cloud economics, data privacy, and cybersecurity. Comprehensive federal legislation with governing guidelines would empower healthcare organizations to move forward with this innovative solution, however, they are challenged by preemption, jurisdiction, judicial cases, private business rights, and private-right-to-action political debates. The US healthcare system has therefore, been without a safety net for the risky decision of cloud migration, and with fear of the unknown there is little movement in this direction. On the flip side, however, tech retail is leading the way to the public cloud and is experiencing massive data breeches and security issues as a result of the boom in Silicon Valley and online shopping. American healthcare leaders will

not proactively adopt a cloud strategy until the US government can reassure them that they will enforce standardized regulation on their behalf. As Rubin writes in his research, there is no specific "cloud law" that guides and governs how industries interact with technologies. There is no direct regulation for cloud services; therefore, healthcare leaders are left to navigate a matrix of different legal and regulatory rules that are as wide as the scope of technology itself (Rubin, 2019). The objective of this study is to examine federal and state court cases in order to understand policy and regulatory challenges and available solutions.

4.2 Problem Statement

Are U.S. healthcare laws and regulations that exist today sufficient to protect healthcare data stored in the public cloud, and if not which gaps remain? It appears that there is insufficient regulatory protection over the use of the public cloud for use in the healthcare industry, i.e., patient data, genomics, electronic medical records, research compute, and clinical workloads. Without regulations from the United States legislative branch, healthcare data and corporations are at risk of a serious threat to our national security. Countries in Europe and India have recently made serious regulatory changes in order to protect healthcare data by passing such laws as the DISHA (India, 2018) and the General Data Protection Regulation (European Union, 2018).

The following questions are the focus for this study: (1) What are the current regulations and laws pertaining to healthcare and the use of the public cloud? (2) What are the current court cases (both state and federal) that pertain to public cloud providers regarding healthcare data, privacy, and use? (3) What are the gaps in the requirements that need to be met for hospital CIO's to move their data and workloads into the public cloud safely?

4.3 Methods

The research is a qualitative study that consists of a legal case study, and expert reviews of the legal cases with four Hospital System Chief Information Officers regarding their thoughts and impressions of healthcare data/workloads running in the public cloud.

4.3.1 Instrumentation and Data Collection

One set of interview questions was designed and used to interview a minimum of four hospital/healthcare CIO's. Using a convenience sample, the hospital CIO's were selected based on the size of their hospital systems, diversity of patient population, hospital type, and geographic location. Four CIOs were interviewed to optain an expert opinion, representing a childrens hospital, two university hospital systems, and one for profit hospital systems.

Five open-ended interview questions that were all designed to allow the executives to elaborate where they desired. Questions were piloted prior to the interviews through feedback from field experts in healthcare IT and modified to fit the objectives of the study.

4.3.2 Data Analysis

An inductive thematic analysis of the qualitative data guided the development of a CIO Cloud Checklist A preliminary coding structure will be inductively developed based on the recommendations from the literature and legistlation. Key informatant interview trasnscripts were systematically read to identify emerging categories and to identify gaps that are not captured in the literature (Brooks J, 2015). Codes were grouped to form themes that guided the creation of the checklist items.

4.4 Results

4.4.1 Legal Case Study Results

Eight legal cases were reviewed and their findings summarized below. The intent of the reviews below were to highlight the lessons learned and outcomes of the legal cases in order to contribute to guidance and considerations for CIO's who are investigating moving their healthcare data into the public cloud.

The first and most recent legal case on is a lawsuit between SalusCare, a behavioral healthcare provider based in Florida who brought suit against Amazon Web Services (AWS) due to a cyberattack that occurred in March of 2021 that resulted in mental health, addiction, and financial patient data accessed via Microsoft Office 365 account and stored in a Ukraine based AWS S3 storage bucket. SalusCare is suing Amazon in order to gain access to the audit logs, as well as, asking for the permanent disabling of the S3 storage buckets. The fact that AWS is unwilling to share audit logs is troubling to a CIO moving to the public cloud, because IT specialists use audit logs to conduct investigations on hardware and software issues. Additionally, the cyberattack was accessed via Microsoft's public cloud and then stolen data was put into Amazon's public cloud (HIPAA Journal, 2021).

The second legal case, was a class action lawsuit brought by Illinois residents on December 17, 2019 against Amazon Web Services and Pindrop for violations of the Biometric Information Privacy Act alleging that AWS collected, possessed, redisclosed and profited from failing to safeguard the plantiffs biometric identifiers, and biometric information. John Hancock, financial services contracted AWS and Pindrop to provide voice recognition services and John Hancock, stored the data on AWS servers. For this reason, the court ruled in favor of the

defendant's AWS and Pindrop, since the data was not their's and they were only doing what John Hancock had contracted them to do.

The lesson learned from for CIO's in this case, is that when contracting a public cloud provider, the data and any actions upon the data that could be considered harmful by the persons who originate the data is still the responsibility of the healthcare organization. Healthcare CIO's should be take care that they do not assume a zero risk model when transferring data management over to a public cloud provider (McGoveran v. Amazon Web Servs., Inc., 2020).

The third legal case, was filed in December of 2018 by Optum against Amazon Joint Venture to stop the hiring of a former UnitedHealthcare executive who allegedly stole patient data from the public cloud in order to share strategic product information developed off of patient data with his new leadership. While there is not a direct breach of healthcare data or cloud cyberattack that outlines a weakness in cloud migration – this legal case does bring concern to the value of patient data in the market place as well as, the ease at which it can be accessed and shared (Abelson, 2019).

The fourth court case, is a lawsuit in a French court that was brought against Microsoft (MSFT) Azure by the Conseil National du Logiciel Libre which explicitly prohibit MSFT's Health Data Hub from transferring personal data to third countries outside the Europeon Union (EU). By transferring personal data outside of the EU, MSFT violate the GDPR in light of *Schrems II*. The importance of this legal case is the need to put an end to unlawful interference with the right to privacy and the protection of personal data. Healthcare CIO's should take data sharing with third parties, hosting data offshore, and violation of privacy laws into consideration when evaluating the use of the public cloud (Zannotti, 2020).

The fifth legal case reviewed, is the class action lawsuit filed against Amazon, Google (Alphabet) and Microsoft by Illinois residents in July of 2020 for violation of the Biometric Information Privacy Act, when their personal photos were used by the three public cloud companies above to train their facial recognition technologies without obtaining the subjects' permission. The court has not yet ruled on this case, however, seeing that the data was gathered by the cloud providers and shared with IBM's Artificial Intelligence tool – IBM commented that the user could opt out of the data sharing in their flikr application.

A healthcare CIO should review this case in terms of their continued responsibility to safeguard healthcare data even when using public cloud providers for their data storage/compute needs. Due to a lack of law's that in turn hold CSP's accountable, the corporation where the data originates – where the user/patient shared the data is held responsible (STEVEN VANCE and TIM JANECYK v. INTERNATIONAL BUSINESS MACHINES CORPORATION, 2020).

The sixth case reviewed is a data privacy lawsuit brought against the University of Chicago Medical Center and Google by a patient named Matt Dinerstein, which demonstrates the increase in patient data sharing between hospital systems and public cloud providers. The case argues that in 2017, Google in a partnership with the University of Chicago intended to create machine learning tools that would predict patients' future health problems and adverse medical events. In order to complete this join venture, the university handed over five years of "de-identified" electronic medical record data to Google – Matt Dinerstein's data was amongst the records.

Recently the Illinois court dismissed the case, because Dinerstein did not prove damages. A hospital CIO, should be cautious though, that as laws are discussed and legislation is

developed in these areas, that the hospital system could be looked at as responsible and liable for patient data that is shared without the patient's knowledge and permission (Matt Dinerstein v. Google (Alphabet), 2019).

The seventh case that was reviewed was a congressional inquiry about the illegal sharing of patient records between Ascension Health and Google in December 2019. The partnership led to the inquiry and criticism from patients and lawmakers because of the potential violation of Health Insurance Portability and Accessibility Act (HIPAA) as Google employees will now have access to patient records without the approval of the patients. The congressional inquiry has asked the healthcare system to provide proof that they provided advance notice to paients about the deal and if they were given an opportunity to opt-out of the data sharing.

The take away for CIO's in this congressional inquiry is that all partnership's where patient data is being shared, even de-identified data, should be shared with the originator of the data in order to obtain informed consent. All hospital leadership should be conscious of patient rights in their business decision making (Landi, Fierce Healthcare, 2019).

The eighth and final legal case reviewed was again involving Google (Alphabet) where they face a five million dollar privacy lawsuit for illegally tracking the internet use of their users even whent the user is browsing in the "private" mode which is equal to opting out of their data sharing. According to the complaint filed in the federal court in San Jose, California, Google gathers data through Google Analytics, Google Ad Manager and other applications and website plug-ins, including smartphone apps, regardless of whether users click on Google-supported ads. Google "cannot continue to engage in the covert and unauthorized data collection from virtually every American with a computer or phone," the complaint said.

This legal suit is a warning that as we grow the internet of medical things, and devices across all hospital systems, there is a responsibility to protect the patient data and the patient's privacy. Hosptial corporations should take care to insure that they are only partnering with those cloud service provider's that are protecting patient rights (Stempel, 2020).

Legal Case	Lesson Learned
1. SalusCare v. Amazon Web Services	AWS would not share audit logs from a breach. AWS would not agree to permanently shut down hacker's access to S3 storage.
2. Congressional Inquiry into Accession and Google's joint venture	Sharing patient information without the knowledge or permission of the patient.
3. Google vs. class action	Illegally tracking a user's internet activity while they were in private mode.
4. University of Chicago Medical Center and Google vs. Matt Dinerstein	Patient data, medical records shared without patient's permission or knowledge.
5. Steven Vance & Tim Janecyk v. Microsoft	Biometric data sharing without patient permission or knowledge
6. Conseil National du Logiciel Libre vs. Microsoft	Illegally sharing patient information offshore
7. Amazon, Google (Alphabet) & Microsoft vs. Illinois residents	Biometric data sharing without patient permission or knowledge

8. Optum vs. Amazon Joint Venture	Stealing and sharing of patient/healthcare information for competitive advantage

4.4.2 Interview Results

The general conscensus of the expert interviews that were conducted with hospital CIO's were that their hospital systems were not storing healthcare data in the public cloud, and although they were exploring the business cases for where it made sense to use the public cloud, they all felt that it was too early right now in their journey to move all of their infrastructure to the public cloud. Out of the four hospital systems, two were the furthest along with a strong Microsoft Azure Cloud relationship. According to one CIO, if there are workloads and data that do not need to be in the public cloud, due to cost savings, the information will be kept on premise in a private cloud. However, he stated, "…there needs to be integrations between the two [public and private cloud] and do the integrations open up holes that I'm now exposing new vulnerabilities into things that I was just trying to protect? Also, according to another CIO, "…I would be hard pressed to find any major health care organization who's primarily running their core infrastructure out of the cloud... it may be [their ambition]".

The requirements to move to the public cloud varied with each level of expertise and knowledge that the CIO or CTO possessed about their organization's legal practices, their current public cloud aspirations, or their experience in working with a CSP. There was a consensus that a state by state law would not be a good thing and that if legislation came out it would need to be federal. Two of the interviewees were more in favor of a certification for CSP's that met all the requirements for healthcare organizations to confidently move data to the

cloud whereas, the other two interviewees felt that a law that could be enforced would be best. According to one CIO, he does not want another unfunded mandate, like the Meaningful Use Act forcing his hospital system to incur additional costs in order to be compliant with the law. Unanimously, all of the interviewees did not want their healthcare data to leave the continental United States – as they saw this as a risk in partnering with a CSP. Lastly, there was a strong theme with all CIO's to conduct a vendor deep dive, to include legal reviews, financial risk modeling and privacy/security compliance reviews.

The common fear or reason for resistance when adopting public cloud technologies, was the loss of control of their healthcare data. One concern was what would happen if the vendor relationship was terminated, to the data/information stored in the CSP's datacenter - "…you're a business and they just shut you off, you're down. You're like, wow, now what do we do?". Another concern was "…how do I get my data out at the end of this when we divorce? Having that in the contract at the front end and having it be something which is actually doable". And to pile on further, another issue was stated as, "I'd be worried that… losing control and not being able to have a capability to restore services in a time frame that would be expected from my community". One CIO summarized this best when he described the difference in control between keeping his data on premise or putting it in the public cloud,

> …if I've got something that I'm implementing on premise, I know how I'm protecting it… I know what kind of firewalls I have around it. I know what kind of backups… [but] when I put something in a cloud provider, I'm just trusting they're doing the right stuff because, you know, it's not like I can go… get in a car and drive up to Arlington, Virginia, and demand to be allowed to look at my data.

Healthcare CIO's lead hospitals in the adoption of the public cloud and their opinions are important for the industry to watch for trends.

4.5 Discussion

The public demand to be cloud ready is not slowing down and healthcare as a whole is being forced to catch up. Without swift, bipartisan government regulation to protect healthcare organizations and the patients/beneficiaries, significant data compromise is inevitable. Healthcare leadership will be forced by economics and the competitive landscape they face to move their operations into the cloud and will do so taking on significant risk. The experts in delivering health outcomes and medical decisions cannot face the burden of deciphering legalese and cyber speak. The US government must step in and protect its citizens and businesses. Organizations often implement more than one cloud solution from several cloud vendors for storage or application development. Each cloud service provider and subcontractor is obligated to submit to a Business Associate Agreement (BAA). Any cloud vendor that handles PHI is required to protect it to HIPAA standards which is an intimidating notion, especially if an organization is working with multiple cloud vendors. One of the biggest drawbacks to cloud adoption in the healthcare industry is involving external cloud partners, according to the authors of the BioMed Central report.

However, HealthITSecurity.com reported that cloud service providers that equip proper security for PHI have "little liability risk as a business associate," meaning that a majority of cloud service providers maintain security on par with HIPAA standards (Kail, 2017). Congress needs to establish a unified public cloud operation model and the associated legal framework that healthcare operators should work within. Until this prescriptive and directed solution is outlined with legislation, healthcare executives will continue to see hesitance in cloud adoption and better

availability of data to healthcare providers. The COVID-19 pandemic of early 2020 highlights to the American people, the federal government, and our legislators that a rapidly expandable, scalable solution to track, investigate, and research complex healthcare issues in a timely manner is as critical to our nation's infrastructure as our National Highway System. Technologies like public/private cloud and sophisticated security solutions that evolve and improve daily are the path we must champion to make uninterrupted, expedited data delivery to decision makers and healthcare providers alike. Perhaps the momentary dip in our national economy will be overshadowed by this opportunity to highlight for our elected officials this critical need and this pandemic will be the catalyst for healthcare cloud expansion and, finally, legal framework to surround it (Dignan, 2019). Without strong reform to secure our nation's cyberspace, more harm than good can result by using the public cloud to transform healthcare.

4.6 Limitations

Some limitations that are worth noting for this study, were COVID19 restrictions in regards to interviewing hospital leaders, and access to legal cases. Due to the number of legal cases that were settled outside of court by large tech companies and the number of cases that were dismissed, there is a belief that the actual court cases is much higher than what this study was able to find.

Researchers and legislators should take a deeper look into how the laws today can be revised in order to share the risk and responsibility of patient data monitoring/control between the hospital system and the cloud service provider. Legal cases today do not hold CSP's accountable as much as they are holding the hospital system accountable. Additionally, a comparison of success with privacy laws in other countries and the laws in the United States would be helpful for lawmakers to understand.

4.7 Conclusion

The results of both the legal case reviews and expert CIO interviews are compiled into the checklist below. The key areas were hospital CIO's should ensure that they review/validate a Cloud Service Provider prior to moving to their patient/healthcare data to the public cloud are: legal review, financial review, and data - control, location, access, ownership, management, location, format, security, privacy. As well as, complete the financial and business shared risk model. It is also, important that when making these decisions that the CIO seek the Hospital's board approval or acknowledgment of the decision in order that all parties are aligned and in concert with partnerships.

As more and more hospitals are leaning on Cloud Service Providers (CSP) to bridge the gap in technology advancements, there is a strong need for hospital leadership to have the right tools in the hands of the decision makers.

Figure 3: Checklist for Moving Healthcare Data and Workloads to the Public Cloud

- Complete A Legal Review
    - Does vendor carry cyber insurance?
    - What is liability for data breaches, etc?
    - Is there a BAA in place?
    - Are there cloud Terms of Service in place?
    - What are the Service Level Agreements?
    - What are data ownership policies?
    - What defines a subcontractor and third party associate, etc?
- Complete A Financial Review

    - What is the consumption/cost model?
    - What are the egress fees?
    - What penalties apply if early contract termination?
    - What are penalities for SLA's?
    - Complete financial risk model – opex/capex, ROI versus TCO
- Complete A Data Privacy Review
    - Where is the data stored – multiple locations, overseas?
    - What is the data segregation plan?
    - What is the auditability process for all data?
    - Are all privacy laws followed/compliance met by the CSP?
- Complete A Data Security Review
    - What is the Data Management plan/policy?
    - What certifications does the vendor have for cloud and security operations?
        - FEDRAMP, Hitrust, ISO, FSMA, etc.
    - What is the data format (containers, cloud native, virtual machines, archival)?
    - What is the vendor's process for recoverability and reliability?
    - Does CSP have a continuity of operations plan?
    - Does CSP have cybersecurity protocol/polices they can share?
- Complete A Data Access Review
    - Who all has access to the data? Are there any third parties?
    - Can data be copied or downloaded?
- Complete A Vendor Stability Review

    - Vendor Deep Dive - share the vendor's business profile, history, relationships, finances, etc with the hospital board for approval?
- Complete A Vendor Termination Plan
    - Who can terminate the relationship and when?
    - What happens to the data in the event that there is a vendor termination?
    - What are notification timelines, processes for termination?
- Complete A Risk Model Evaluation
    - Completion of risk model with board of hospital executive review and approval?
        - What is the risk of loss of data control to the hospital?
        - What is the risk of cyber threats and data loss/deletion?

5 CHAPTER V REFERENCES

Abelson, R. (2019, Feb 1). Retrieved from New York Times: https://www.nytimes.com/2019/02/01/health/unitedhealth-amazon-chase.html

Allen, M. (2018). Health insurers are vacuuming up details about you. That could raise your rates. *ProPublica - Health*, 1-2.

Amazon Web Services. (2019, July 30). *Security*. https://aws.amazon.com/security/" https://aws.amazon.com/security/

American Hospital Association. (2019, January 1). www.//aha.org

Arango, S. (2019, 13 July). *The Third-Party Doctrine in the Wake of a "Seismic Shift"*. American Bar: https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2019/third-party-doctrine-wake-of-seismic-shift/

Boone, M. (2019, July 15). *The Pros and Cons of Cloud Computing for Healthcare*. Retrieved from CyberlinkASP: https://www.cyberlinkasp.com/pros-cons-cloud-computing-healthcare/

Breeden II, J. (2017, July 25). *A Tool That Can Keep Federal Data Centers Safe Amid Cloud Chaos.* Retrieved from Nextgov: https://www.nextgov.com/ideas/2017/07/tool-can-keep-federal-data-centers-safe-amid-cloud-chaos/139700/

Brookings. *How will a national data privacy law affect connected devices, applications, and the cloud?* (2019, 16 September). https://www.brookings.edu/events/how-will-a-national-data-privacy-law-affect-connected-devices-applications-and-the-cloud/

Brooks J, M. S. (2015). The Utility of Template Analysis in Qualitative Psychology. *Qualitative Resseach Psychology*, 202-222.

Carter, A. (2019). Considerations for Genomic Data Privacy and Security when Working in the Cloud. *American Society for Investigative Pathology and the Association for Molecular Pathology.*

Centers for Disease Control. (2019, July 28). *Public Health and Promoting Interoperability Programs.* Retrieved from Centers for Disease Control and Prevention: https://www.cdc.gov/ehrmeaningfuluse

Clear Data. (2019, July 31). *HIPAA compliance in the public cloud: You don't have to pilot it alone*. Retrieved from Clear Data: https://www.cleardata.com/news/hipaa-compliance-in-the-public-cloud-you-dont-have-to-pilot-it-alone/

Centers for Medicare & Medicaid Services (2020, March 11). *HHS Finalizes Historic Rules to Provide Patients More Control of Their Health Data.* https://www.cms.gov/newsroom/press-releases/hhs-finalizes-historic-rules-provide-patients-more-control-their-health-data

Columbus, L. (2014, July 17). *Forbes*. Retrieved from 83% Of Healthcare Organizations Are Using Cloud-Based Apps Today: https://www.forbes.com/sites/louiscolumbus/2014/07/17/83-of-healthcare-organizations-are-using-cloud-based-apps-today/#488af69c3b72

Davis, J. (2019, February 15). *Government Report Finds China Could Use Medical Data for Blackmail.* Retrieved from Health IT Security: https://healthitsecurity.com/news/government-report-finds-china-could-use-medical-data-for-blackmail

Davis, J. (2020, December 10). *UPDATE: The 10 Biggest Healthcare Data Breaches of 2020*. Retrieved from Health IT Security: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020

Dignan, L. (2019, August 15). *Trifacta*. Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud; IBM makes hybrid move; Salesforce dominates SaaS: https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-google-cloud-ibm-makes-hybrid-move-salesforce-dominates-saas/

Drees, J. (2019, June 13). *Becker Hospital Review* . Retrieved from Sutter Health sued for allegedly sharing patients' health data with Facebook, Google: https://www.beckershospitalreview.com/cybersecurity/sutter-health-sued-for-allegedly-sharing-patients-health-data-with-facebook-google.html

Eddy, N. (2019, February 8). *5 Cybersecurity threats healthcare faces in 2019 and beyond.* Retrieved from Healthcare IT News: https://www.healthcareitnews.com/news/5-cybersecurity-threats-healthcare-faces-2019-and-beyond

Fahey, S. (2019). The Democratization of Big Data. *Journal of National Security*, 326-331.

Gavriloc, G., & Trajkovik, V. (2012). Security and Privacy Issues and Requirements for Healthcare Cloud Computing. *ICT Innovations*, 143-152.

Geneva Centre for the Democratic Control of Armed Forces.. (2005, November). https://issat.dcaf.ch/download/17202/201862/bg_national-security%20(1).pdf

Grance, W. J. (2011). Guidelines on Security and Privacy in Public Cloud Computing. *NIST Special Publication 800-144*, 4.

Harshbarger, J. A. (2011). Cloud Computing Providers and Data Security Law: Building Trust with United States Companies. *Journal of Technology Law & Policy*, 230-256.

Haufe, K., Dzombeta, S., & Brandis, K. (2014). Proposal for a Security Management in Cloud Computing for Health Care. *Scientific World Journal*.

HealthIT.gov. *Health IT Legislation*. (2020, April 17). 21st Century Cures Act. https://www.healthit.gov/topic/laws-regulation-and-policy/health-it-legislation

HIPAA Journal. (2021, March 26). *HIPAA Journal*. Retrieved from SalusCare Take Legal Action Against Amazon : https://www.hipaajournal.com/saluscare-takes-legal-action-against-amazon-to-obtain-aws-audit-logs-to-investigate-data-breach/

Hoover, J. N. (2013). Compliance in the Ether. *Journal of Buisness & Technology Law*, 256-275.

House Committee on Oversight and Reform. *To the Cloud! The Cloudy Role of FedRAMP in IT Modernization*. (2019, July 17). https://oversight.house.gov/legislation/hearings/to-the-cloud-the-cloudy-role-of-fedramp-in-it-modernization

Jansen, W. (2011). Cloud Hooks: Security and Privacy Issues in Cloud Computing. *In Proceedings of hte 44th Hawaii International Conference on System Sciences*.

Justice, U. D. (2019, April). Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the Cloud Act. *White Paper*. Washington, D.C. , United States: US Dept of Justice.

Kail, M. (2017, July 21). *The top three approaches for improving cloud migration and security*. Retrieved from Cloud Tech: https://cloudcomputing-news.net/news/2017/jul/21/top-three-approaches-improving-cloud-migration-and-security/

Kavita M. Berger, P. A. (2019). National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data. *Front Bioeng Biotechnol*.

Kent, S. (2019). *Federal Cloud Computing Strategy.* Washington, D.C. : Executive Office of the President of The United States.

King, J. (2019, February 11). Cloud Computing Forum. *Industry Snapshot*. Orlando, Florida, USA: HIMSS MEDIA.

Kissel, R. (2019). NIST IR 7298 Revision 2. *Glossary of Key Information Security Terms*.

Kleyman, B. (2018, February 14). *How Does HIPAA Compliance Apply in the Healthcare Cloud?* Retrieved from Health IT Security: https://healthitsecurity.com/news/how-does-hipaa-compliance-apply-in-the-healthcare-cloud

Landi, H. (2019, Dec 9). *Fierce Healthcare*. https://www.fiercehealthcare.com/tech/house-democrat-presses-google-health-data-collection-wake-ascension-deal

Lebeda, F. J., Zalatoris, J. J., & Scheerer, J. B. (2018). Government Cloud Computing Policies: Potential Opportunities for Advancing Military Biomedical Research. *Military Medicine*, e438-e447.

MacDonald, N. (2019). *Market Guide for CLoud Workload Protection Platforms.* Stamford: Gartner.

Majumder, M. A. (2018). United States: law and policy concerning transfer of genomic data to third countries. *Human Genetics*.

Matt Dinerstein v. Google (Alphabet), 1:19-cv-04311 (THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION 6 26, 2019).

McGillivray, K. (2016). FEDRAMP, COntracts and the US Federal Government's Move to CLoud Computing: If an 800-pound gorilla can't tame the cloud, who can? . *The Columbia Science & Technology Law Review*.

McGoveran v. Amazon Web Servs., Inc., Case No. 3:20-CV-31-NJR (Third Judicial Circuit in Madison County, Illinois 9 18, 2020).

Microsoft Corporation, Plantiff v. United States Department of Justice, et.al., Defendants, C16-0538JLR (United States District Court Western District of Washington at Seattle August 29, 2016).

Mohammed Naveed, e. (2018). Privacy in the Genomic Era. *ACM Comput Survey*, 5-8.

Murphy, E. (2013). The Politics of Privacy in the Criminal Justice System: Information Disclosures, the Fourth Amendment, and Statutory Law Enforcement Exemptions. *Michigan Law Review*.

National Sercurity Agency. (2018, August 29). *Cybersecurity Information* . Retrieved from National Security Agency: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-cloud-security-basics.pdf?v=1

O'Dowd, E. (2020, April 17). *Understanding HIPAA-Compliant Cloud Options for Health IT*. https://hitinfrastructure.com/features/understanding-hipaa-compliant-cloud-options-for-health-it

Raja, N. J. (2013). What do they really know about me in the cloud? A comparative law perspective on protecting privacy and security of sensitive consumer data. . *American Business Law Journal*, 413-482.

Rouse, M. (2012). *Definition: Cloud Computing*. https://searchcloudcomputing.techtarget.com/definition/cloud-computing

Rubin, L. (2019, May 29). *Cloud computing and regulation: Following the eye of the storm*. Retrieved from DCD: https://www.datacenterdynamics.com/en/opinions/cloud-computing-and-regulation-following-eye-storm/

Sandru, D.-M. (2020). Tipologia protectiei datelor cu caracter personal in situatii de criza medicala coronavirus COVID-19. *Pandectele Romane*

Snell, E. (2017, August 21). *4 Benefits and Barriers in Utilizing Healthcare Cloud*. Retrieved from Health IT Security: https://healthitsecurity.com/news/4-benefits-and-barriers-in-utilizing-healthcare-cloud

Stempel, J. (2020, June 2). https://www.reuters.com/article/us-alphabet-google-privacy-lawsuit/google-faces-5-billion-lawsuit-in-u-s-for-tracking-private-internet-use-idUSKBN23933H

STEVEN VANCE and TIM JANECYK v. INTERNATIONAL BUSINESS MACHINES CORPORATION, 1:20-cv-00577 (UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF ILLINOIS EASTERN DIVISION 9 15, 2020).

University of Illinois. (2020, January 10). https://cloud.illinois.edu/types-of-cloud-computing-private-public-and-hybrid-clouds/

Weiss, S. (2020, April 1). *Moving to online and telephone-based health services*. https://www.ruralhealthinfo.org/topics/covid-19/innovations

Tech Target.*What is hybrid cloud? Everything you need to know*. (2020, December). https://searchdatacenter.techtarget.com/definition/workload

The Guardian. (2020, February 10). *Amazon wants to question Trump over loss of $10bn 'war cloud' contract*. https://www.theguardian.com/technology/2020/feb/10/amazon-trump-war-cloud-lawsuit-pentagon#maincontent

Y.Tony Yang, K. B. (2012). Regulatory Privacy Protection for Biomedical Cloud Computing. *Beijing Law Review*, 145-151.

Zannotti, P. N. (2020, October 22). *JD Supra*. https://www.jdsupra.com/legalnews/french-court-refuses-to-suspend-61424