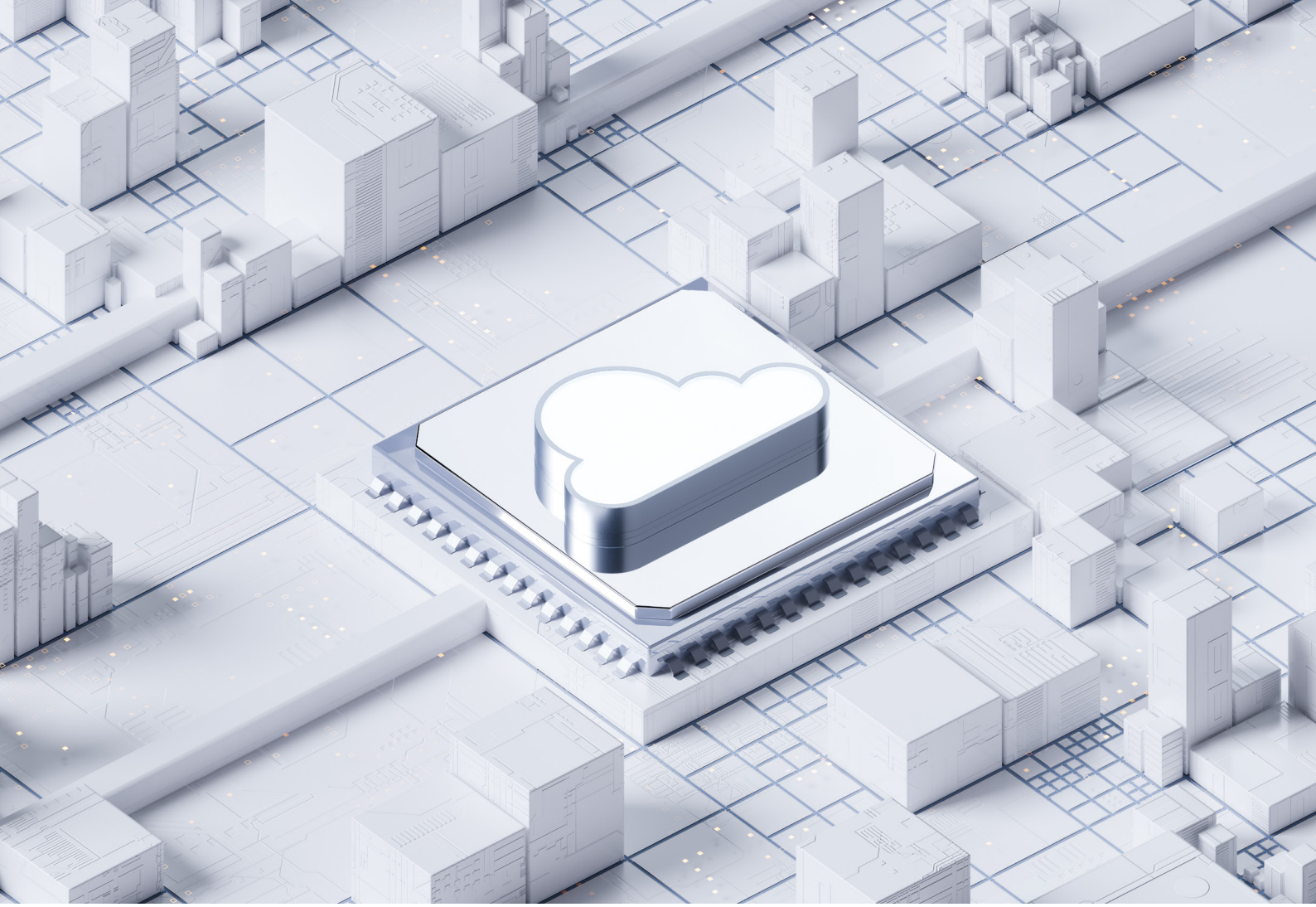
How Healthcare Companies can take Advantage of **Cloud computing** without Sacrificing **Security** or **Compliance**

Lumen21



Introduction

Companies in the healthcare industry need to understand the benefits as well as risks when planning a move into cloud computing. They need to set meaningful expectations with their cloud provider and fully understand what the cloud provider offers in terms of compliance and security. Cloud deployment models (private, public and hybrid) as well as models of service delivery, whether Infrastructure as a **Service (IaaS), Platform as a Service (PaaS),** or **Software as a Service (SaaS),** need to be taken into consideration.

In the first section of this white paper we'll discuss the benefits of cloud computing and IT trends in the healthcare industry which can be effectively addressed by cloud computing when compared to traditional IT areas.

In the second section, we'll discuss the hindrances to cloud computing adoption for the healthcare industry, with a focus on the important compliance requirements for security and privacy that need to be addressed. In the third section, we'll examine the key security issues healthcare organizations need to consider when moving to cloud computing.

Finally, we will talk about how the Common Security Framework can address the security and compliance requirements of the healthcare industry in a cloud environment. More than 84% of hospitals and health plans, as well as many other healthcare organizations and business partners, use the CSF, making it the most widely adopted security framework in the industry.

I. Benefits of Cloud Computing for Healthcare

The availability of data is crucial to patient satisfaction and development of clinical outcomes. **Cloud technologies can help improve the availability of data irrespective of where the patient and clinician are located. The secure sharing of data can also improve the efficiency of treatment authorization and payment processes, both critical to the healthcare system.** Healthcare centers such as clinics and hospitals need quick access to patient data, and this data often needs to be shared with other providers, payors, business associates, and patients. **Cloud technology helps to reduce the burden of sharing data with others who use different processes or media,** enabling healthcare organizations to improve their services, efficiently disseminate the information and reduce delays.

Cloud computing can benefit healthcare in many ways

Clinical Research

The growing usefulness of big data analytics in research and the resulting explosion of data makes cloud computing a crucial aspect of research and development. For instance, a pharmaceutical company may not have the capacity for intensive computing such as DNA sequencing since the amount of data can overwhelm normal computers. Thus, pharma-specific clinical research cloud offerings have been developed to help reduce the cost as well as development of new drugs.

Electronic Medical Records

Cloud-based medical records as well as medical image archiving services are currently being employed by hospitals and healthcare providers. These cloud based services help to offload resource-intensive tasks from the IT departments of healthcare centers thereby giving them the ability to support other imperatives like improvement of clinical support systems and the security of medical devices.

Collaboration Solutions

Solutions that allow video conferencing for specialist consults or remote physician assistance for disaster response is increasingly available due to widespread wireless broadband and smartphone technologies. These solutions are enabled by cloud technology and improve team-based care delivery.

Telemedicine Capabilities

The increasing availability of mobile and cloud technologies has sped the growth of telemedicine, allowing the rapid exchange of electronic health records, online physician visits, and medical devices that provide home monitoring of patient status.

Big Data

Cloud computing helps healthcare companies to save on hardware and managements costs incurred for the local storage of large amounts of data. The cloud accommodates huge data for EHRs, radiology images as well as genomic data for clinical drug trials.

Analytics

Cloud computing makes available the most current, complete insights as well as clinical expertise for supporting healthcare providers' decision-making and helps in improving patient outcomes. Data contained

in the cloud can be analyzed, providing information on treatments, performance, and costs. Results from increased analytics can then be acted upon to provide quality healthcare delivery.

Security

The high incidence of breaches in the healthcare industry is due to a number of causes: the dependence on legacy computer systems that can't incorporate needed security controls, the need to ensure data is immediately available to a variety of users to prevent delays in patient care, the high value criminals place on healthcare data, and the challenge and cost of implementing security controls in the diverse environment in which healthcare operates all contribute to the problem. **Moving to a cloud environment can allow a company to benefit from security controls and processes that are implemented within the cloud for the benefit of all customers, including system currency, patching, network controls, log management, and access control.** This can improve the organization's overall security posture while freeing IT staff to focus more on supporting the business needs that affect patient outcomes.

II. Challenges to Leveraging Cloud Computing for Healthcare

Despite the significant benefits of cloud computing in healthcare delivery, there are barriers that slow down its adoption.

Privacy and Security Regulations

Data stored in the cloud often contains confidential information such as **Protected Health Information (PHI), Personally Identifiable Information (PII)** and **Payment Card Industry information (PCI)** that is subject to state and federal regulatory requirements for safeguards to prevent misuse. Contractual requirements regarding data jurisdiction, required security controls, and privacy regulations are concerns that affect the adoption of cloud computing by healthcare organizations.

Global Challenges Related to Data Privacy Legislation

Governments of different countries are battling with the challenges of addressing and coordinating the needs of privacy and freedom of data. Since the data location is often abstracted in cloud computing, a cloud service provider can easily move data between different countries without the knowledge of the data owner. This means data may be located in multiple countries, each having a different legal approach to privacy. This concern must be addressed prior to moving data to the cloud.

Service Reliability

While cloud service providers offer strong service level agreements and often have more robust solutions for reliability and availability than on-premise systems, some widely reported cloud vendor outages have affected a large number of businesses. Even if the cloud environment is available, organizations may incur a connectivity outage that prevents access to the data. The dependence of the healthcare sector on the availability and reliability of information is often a matter of life and death. These applications often need to meet very high performance and reliability standards.

Cloud Management Skills

Architecting a secure, functional, and stable cloud environment requires a skill set that is new for many IT staffers. They may not have the skills to properly design a robust, redundant, and secure cloud environment. Managing the environment on a daily operational basis takes an additional skillset. IT teams are often reluctant to move to a cloud environment because they don't know if they can build and support cloud systems such that they will meet the business requirements.

Legacy Systems

Many healthcare companies have legacy applications that are critical to business operations. Organizations

struggle just to integrate these legacy systems with new applications. Moving them to a cloud environmentcan be very challenging and may introduce risks to business stability.

Risk Assessments and Audits

Regulatory compliance requires regular risk assessments that create **an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information.** Identifying the threats, vulnerabilities, and risks in the cloud environment can add challenge to the process. In addition, customers and regulators require regular audits of the security controls in place to protect data.

III. Cloud Computing in Healthcare: Key Security Issues

Cloud computing efficiencies can reduce IT costs in healthcare, but only if the vendors offering cloud computing are prepared to satisfy the privacy and security requirements set by HIPAA.

As healthcare providers consider adding new applications on a tight budget and without having the required resources, the option of cloud computing is appealing.

Healthcare organizations that are considering cloud computing must consider data security and availability risks before making the final decision. They should take the necessary steps to implement the appropriate controls to meet regulatory compliance. HIPAA compliant cloud computing is possible by addressing these challenges.

Cloud Identity and Access Management

Traditional identity management based on unique usernames and passwords may not provide adequate security in a cloud environment. Strong centralized access controls using two-factor authentication may be required.

Data Protection

Encrypting both data at rest and data in transit provides an additional level of protection to the cloud environment. Encryption provides a Safe Harbor under the HITECH Breach Notification Rule to reduce the risk of a data breach. Encryption is only as strong as the security of the encryption keys, however. The encryption solution should include key management that allows the customer to decide whether they want to control all or part of the encryption key (using split-key management, for example), of if they want the vendor to securely manage the encryption keys on their behalf.

Incident Response

Cloud customers are dependent on their cloud provider to respond to security incidents within the cloud infrastructure. Incident notification times should be addressed in a Business Associate Agreement. But healthcare organizations shouldn't rely solely on the cloud provider for incident response. They should have a complementary incident response process that provides remediation as well as service continuity.

Secured Architecture

Additional network controls need to be implemented in the cloud environment to provide the necessary security of healthcare data. Network and application firewalls, anti-virus and malware services, system log monitoring, file integrity services, and other security controls that are not shared with other cloud customers may need to be included to ensure a secure cloud architecture.

Device Management Solutions

While cloud computing can make it easier to share data with authorized users, it can increase the risk of data loss unless the ability to download or store the information is strictly controlled. The use of mobile devices to access cloud-resident data has improved accessibility to this critical data, but also requires the implementation of device management solutions that help ensure that data is not stolen or lost as a result of unsecured devices.

IV. How to Meet Healthcare Compliance Requirements in the Cloud

Ensuring regulatory compliance is always a challenge. The people, process, and technology-based policies and procedures required to meet compliance requirements can be daunting. Implementing requirements can be time-consuming, resource-consuming, and expensive.

Once an organization understands that compliance is an ongoing process, not simply a statement, maintaining the required level of compliance becomes easier. A big step in moving towards compliance as a continuous process is the implementation of the CSF framework.

The CSF framework is based on the ISO 27002 Code of Practice for Information Security Controls and includes the controls that healthcare organizations must implement to comply with HIPAA and HITECH requirements. Framework controls are designed to address risks to the confidentiality, integrity, and availability of protected health information. This set of prescriptive controls provides consistency in the implementation of controls and transparency to customers who rely on the certification to determine whether their providers can adequately protect healthcare data.

Using a cloud provider with a cloud environment like Lumen21, provides a healthcare organization with a clear understanding of the security controls implemented in the environment and confidence in the processes implemented to ensure those controls continue to function as intended.

Conclusion

As healthcare organizations migrate toward new security, reporting, compliance, and technology requirements, organizations are seeing the light in the cloud computing environment. Although the healthcare sector is wary of adopting new technologies, they remain an integral part of the growing cloud movement. The healthcare industry experienced strong growth between 2010 and 2015, during which time cloud services were projected to reach $148.8 billion worldwide. Cloud computing has become more important than ever, especially in healthcare organizations. This can be attributed to the fact that the benefits of cloud computing in providing solutions to the challenges of managing a secure and cost-effective IT environment are becoming more appropriate and critical for healthcare organizations, regardless of their nature and size. This is largely due to the adoption of cloud technology to provide security, compliance and quality of care to the healthcare industry.

Lumen21 is a company that specializes in the area of IT Security and Compliance. Lumen21 has a series of solutions and services for used by Healthcare organizations in order to leverage newer technology while meeting its regulatory and security responsibilities. Lumen21's Compliant Cloud Computing Solution is truly HIPAA compliant and also maps to NIST SP-800-144, NIST SP 500-299 standards as well as it complies with or exceeds the Cloud Security Alliance Framework (CSA). Lumen21 enables the process of compliance and allows a healthcare company the ability to measure, monitor, report and improve that process. Lumen21 offers its O365+ Compliance Service leveraging Microsoft products such as O365 Enterprise, Enterprise Mobility, Device management and Azure Storage, implementing the necessary controls that are configured and monitored to meet regulatory standards. That is why at Lumen21 we believe HIPAA compliance is not a statement, it's a continuous process that is vetted and certified. You can learn more about our solutions that can help you meet regulatory compliance in your It operations as well as enhance your security by reaching out to us at sales@lumen21.com or visit us at www.lumen21.com HIPAA compliance is not a statement, it's a continuous process that is vetted and certified. You can learn more about our solution by reaching out to us at sales@lumen21.com or visit us at www.lumen21.com