HIPAA Compliance in the Cloud: **Addressing the Gaps**

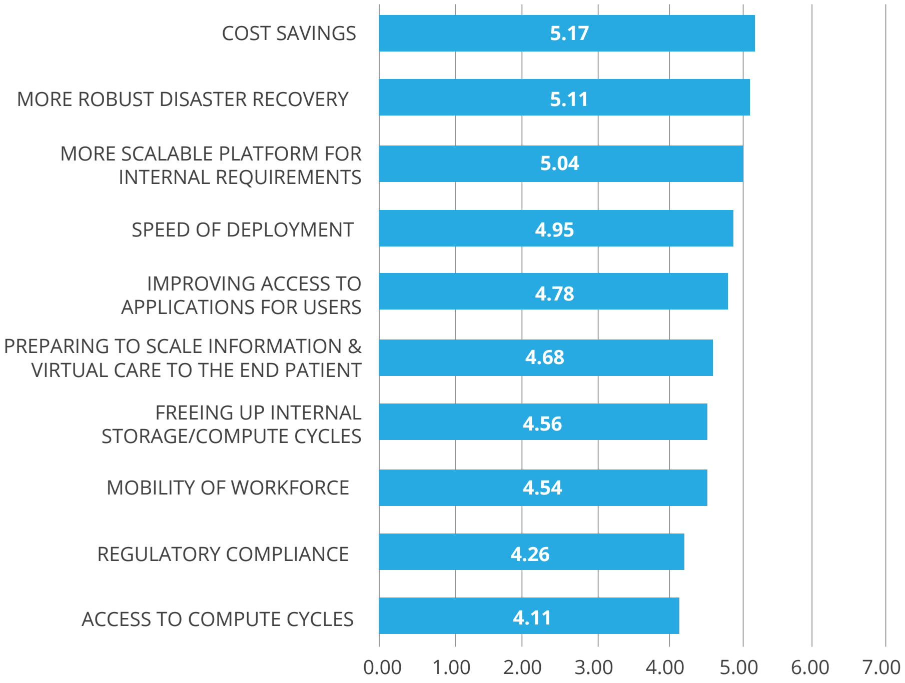
Lumen21

Healthcare organizations, like other industry verticals, face a growing challenge in managing the costs associated with running their IT operations. The growth of data access and storage, demands for 24x7 access to user systems, and the need for continual business innovation all contribute to more need for processing and computing capacity. Although the compute power has continued to accelerate with technological advancements of chip technology, virtualization, and other technologies, infrastructure continues to be expensive, not just to procure, but to operate and maintain.

Cloud technology can help businesses address this challenge. Public cloud vendors can provide a company with computing capacity that can be utilized when computing needs escalate, and can be reduced when needs decline. It's an economical alternative to the on premise, capital intensive IT infrastructure solution that business have been using for quite some time. With the advent of this cloud technology comes additional concerns around security as well as compliance for regulated industries such as healthcare. As a result, healthcare organizations overall have been slower to adopt cloud technology solutions. Security concerns are certainly one reason. After all, patient data is a high value commodity in the black market. Certainly these security concerns are valid, but we believe that the challenge of meeting regulatory compliance also has a great deal to do with the lower adoption rate as well. Cloud providers in general may not do everything that may be needed to meet an individual client's specific compliance and security needs. This can be seen in more detail by looking at a mapping of HIPAA regulations to common public cloud offerings. The cloud offering referenced in this white paper is not from a specific vendor, but it represents a generic offering that is consistent from numerous public cloud vendors.

The reality is that moving to the cloud in some manner is becoming more and more inevitable. IDC estimates that "by 2020, 80% of healthcare data will pass through the cloud at some point in its lifetime as providers seek to leverage cloud base technologies and infrastructure for data collection, aggregation, analytics and decision making." So the cloud may well stop being referred to as public or private according to IDC, "it will simply be the way business is done and it is provisioned." Certainly momentum is there, and a recent HIMSS Analytics 2016 Survey shows that much:

What's behind the move to the cloud?



Rating scale - "1" being a non-motivating factor and "7" being a very motivating factor

The economics and transformational ability of the cloud to assist in the way healthcare is delivered is compelling. At the same time, healthcare organizations may be among the least prepared sectors against cyber-attacks. Healthcare organizations face an estimate of one cyberattack per month while struggling to find effective strategies to keep the systems safe. Recent research from the Ponemon Institute shows that about 48% of the organizations they surveyed had a breach involving loss or exposure of PHI in the past year. They identified the biggest threats as system failures, unsecured medical devices, and unsecured mobile devices. Introduce cloud technology into this mix and it is easy to understand the concern about having systems moved out of the on premise customer environment and on to the open environment of a cloud provider.

But the public cloud environment is very often better run and operated than many on premise organizations can operate their own, including management of their security controls and processes. There can be many reasons for this; they have many more resources that are dedicated to protecting the cloud environment, they have the ability to hire expertise in running these systems, or quite simply they may be better because they have to be better. Running a secure environment is their business, and they serve hundreds of thousands to millions of users. So as Forrester Research points out "If you are resisting the cloud because of security concerns you are running out of excuses."

In addition to the operational excellence and security controls available in the cloud environment, however, the healthcare industry must consider not only security, but also compliance. This dilemma is made more complicated as there are two parts to this equation; the cloud provider portion and the customer portion. The coordination of those parts needs to be addressed in order for healthcare organizations to make the move to the public cloud in a confident, after secure and compliant way.

Cloud as we come to know it tends to be public in nature; one large entity that various users use and share in some way or form. It is this sharing--of data, systems, or access--that is an issue for healthcare organizations. Cloud providers in general have addressed the most common users of cloud consumption, and the model lends itself well to that. Think of it in terms of a bank and a safe deposit box. A bank has a fortified building, with alarms, video cameras, bars, and security personnel, all to protect a very large safe that contains customer's individual safe deposit boxes. The bank, however does not know what the customer puts in the safe deposit box, and does not manage, inventory, or support the customer in how they choose to use their box. Cloud providers operate in a similar way. Certainly among the major cloud providers, they have invested, certified and provide numerous capabilities and features to provide a solid cloud environment for customers to use. They work hard and invest in these capabilities. The customer then installs an application or data into this environment much like a customer would store certain possessions into a safe deposit box inside the bank. Just as with the bank, the cloud providers are not in the business of taking care of the contents of the safe deposit box, but rather the bank environment in which the box resides. This means that if a healthcare customer is going to abide by HIPAA regulations they will have to ensure that not only the bank portion meets regulatory requirements but also the safe deposit box portion does as well or they will not be in compliance. They can't just put applications or data in the cloud and assume all is well. They need to have compliance processes in place to manage the cloud environment, just as they do with the on premise environment. The mapping of HIPAA Regulations below to cloud services can discourage a Customer from moving into the cloud as the needed effort on their part can be complicated, sophisticated, and time consuming. Ultimately, the compliance responsibility will rest with the customer.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
1	**§164.308(a)(1)(i)**	**Required Standard: Security Management Process** Company has implemented policies and procedures to prevent, detect, contain, and correct security violations.	Cloud Vendor: 0% Customer: 80%	The Cloud Vendor is responsible for the infrastructure platforms, including whether they offer services that can be configured to meet the security, privacy, and compliance needs of most customers. However, customers are responsible for their environment after their cloud service has been provisioned. This responsibility includes applications, data content, virtual machines, access credentials, and compliance with regulatory requirements applicable to a particular industry and/or location.	The customer is responsible for providing security policies and procedures for managing the customer's cloud environment according to the HIPAA Administrative, Physical, and Technical Safeguards as well as all customer business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI.
2	**§164.308(a)(1)(ii)(A)**	**Required Implementation Specification: Risk Analysis** Company has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by Company.	Cloud Vendor: 20% Customer: 80%	Customers should determine if the Cloud Vendor services being considered have been audited by independent external auditors under industry standards such as ISO 27001, and review those audits. Customers may wish to perform an individualized risk analysis that examines the anticipated configuration of the Cloud Vendor services they will be using.	The customer is responsible for performing risk assessment activities for the customer's cloud environment as well as for the customer business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI.
3	**§164.308(a)(1)(ii)(B), §164.306(a)**	**Required Implementation Specification: Risk Analysis** Company has implemented security	Cloud Vendor: 0% Customer: 100%	Cloud Vendors should provide a basic, defined set of controls for all customers, as well as provide customers with the ability to implement additional security measures sufficient to	The customer is responsible for identifying and implementing any required security measures for the customer's cloud environment as well as

		measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.		reduce potential risks and vulnerabilities to a reasonable and appropriate level.	for the customer business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI.
4	**§164.308(a)(1)(ii)(C)**	**Required Implementation Specification: Sanction Policy** Company applies appropriate sanctions against Workforce members who fail to comply with the security policies and procedures of Company.	Cloud Vendor: 33% Customer: 67%	Any Cloud Vendor staff who fail to comply with the Cloud Vendor's security policies and procedures should be subject to an investigation process and appropriate disciplinary action up to and including termination.	The customer is responsible for implementing a sanction policy for customer employees.
5	**§164.308(a)(1)(ii)(D)**	**Required Implementation Specification: Information System Activity Review** Company has implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Cloud Vendor: 10% Customer: 90%	Cloud Vendors are responsible only for monitoring the areas of the environment for which they provide direct support. Cloud Vendors may provide access to some logging data for the customer's systems. Customers are responsible for collecting, monitoring, and reviewing logs for their environments.	The customer is responsible for collecting and monitoring logs from all systems supported within the customer's cloud environment, including customer's application-specific logs. Potential issues must be identified, tracked, and resolved.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
6	**§164.308(a)(2)**	**Required Standard: Assigned Security Responsibility** Company has identified the security official who is responsible for the development and implementation of the security policies and procedures of Company.	Cloud Vendor: 33% Customer: 67%	Third party audit documents should provide evidence of management commitment to information security and management responsibility.	The customer is responsible for assigning security responsibility for the company.
7	**§164.308(a)(3)(i)**	**Required Standard: Workforce Security** Company has implemented policies and procedures to ensure that all members of its Workforce have appropriate access to EPHI and to prevent those Workforce members who do not have access from obtaining access to EPHI.	Cloud Vendor: 5% Customer: 95%	Cloud Vendor customers are responsible for managing access to any cloud services and resources they use. Third party audit documents should provide evidence that access control for the Cloud Vendor employees is provided using role-based access and follow the principle of least privilege for access to all vendor environments.	The customer is responsible for authorizing and providing all access to systems and data within the customer's cloud environment, including configuring role-based access that provides minimum necessary levels of access rights. If multi-factor authentication is desired, the customer is responsible for identifying and implementing the appropriate MFA tools.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
8	**§164.308(a)(3)(ii) (A)**	**Addressable Implementation Specification: Authorization and/or Supervision** Company has implemented procedures for the authorization and/or supervision of Workforce members who work with EPHI, or work in locations where it might be accessed.	Cloud Vendor: 33% Client: 67%	Third party audit documents should provide evidence that access to Cloud Vendor assets are granted based upon management authorization and that the Cloud Vendor provides adequate supervision of its personnel.	The customer is responsible for authorization and supervision of all customer workforce members.
9	**§164.308(a)(3)(ii) (B)**	**Addressable Implementation Specification: Workforce Clearance Procedure** Company has implemented procedures to determine that the access of a Workforce member to EPHI is appropriate.	Cloud Vendor: 33% Customer: 67%	Third party audit documents should provide evidence that a background check is performed as part of the hiring process. The background check should validate previous employment, education, criminal records; fingerprinting; required security training; and access approvals.	The customer is responsible for background screening policies and procedures for customer workforce members.
10	**§164.308(a)(3)(ii) (C)**	**Addressable Implementation Specification: Termination Procedures** Company has implemented procedures for terminating access to EPHI when the employment of, or other arrangement with, a Workforce member ends or as otherwise determined by Company.	Cloud Vendor: 33% Client: 67%	Third party audit documents should provide evidence of that the Cloud Vendor Corporate has a standard employee termination process that removes access within 24 hours of termination.	The customer is responsible for termination policies and procedures for customer workforce members.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
11	**§164.308(a)(4)(i)**	**Required Standard: Information Access Management** Company has implemented policies and procedures for authorizing access to EPHI that are consistent with the requirements of the Privacy Standards.	Cloud Vendor: 5% Client: 95%	Cloud Vendor customers are responsible for managing access to any cloud services and resources they use. Third party audit documents should provide evidence that access control for the Cloud Vendor employees is provided using role-based access and follow the principle of least privilege for access to all vendor environments.	The customer is responsible for authorizing and providing all access to systems and data within the customer's cloud environment, including configuring role-based access that provides minimum necessary levels of access rights. If multi-factor authentication is desired, the customer is responsible for identifying and implementing the appropriate MFA tools.
12	**§164.308(a)(4)(ii)(A)**	**Required Implementation Specification: Isolating Health Care Clearinghouse Functions** If Company is a health care clearinghouse and part of a larger organization, Company must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization.	Cloud Vendor: 10% Customer: 90%	The Cloud Vendor should guarantee that data storage and processing is logically segregated among customers of multitenant environments. Segregation controls and prevents the unauthorized and unintended information transfer via shared system resources.	The customer is responsible for identifying any clearinghouse functions that must be segmented within the Cloud Computing environment.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
13	**§164.308(a)(4)(ii)(B)**	**Addressable Implementation Specification: Access Authorization** Company has implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Cloud Vendor: 30% Customer: 70%	Cloud Vendor customers are responsible for managing access to any cloud services and resources they use. Third party audit documents should provide evidence that access control for the Cloud Vendor employees is provided using role-based access and follow the principle of least privilege for access to all vendor environments.	The customer is responsible for authorization of all customer workforce members and any access granted to third parties.
14	**§164.308(a)(4)(ii)(C)**	**Addressable Implementation Specification: Access Establishment and Modification** Company has implemented policies and procedures that, based upon Company's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Cloud Vendor: 30% Customer: 70%	Third party audit documents should provide evidence that access to Cloud Vendor assets is granted based upon management authorization.	The customer is responsible for authorization and review of all customer workforce members and any access granted to third parties.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
15	**§164.308(a)(5)(i)**	**Required Standard: Security Awareness and Training** Company has implemented a security awareness and training program for all members of its Workforce (including management).	Cloud Vendor: 30% Customer: 70%	Third party audit documents should provide evidence that all appropriate Cloud Vendor employees take part in a required security-training program.	The customer is responsible for providing required security training for the customer workforce members.
16	**§164.308(a)(5)(ii) (A)**	**Addressable Implementation Specification: Security Reminders** Company periodically distributes security reminders and updates to its Workforce.	Cloud Vendor: 30% Customer: 70%	Third party audit documents should provide evidence that all appropriate Cloud Vendor employees are recipients of periodic security awareness updates when applicable.	The customer is responsible for providing required security updates for the customer workforce members.
17	**§164.308(a)(5)(ii) (B)**	**Addressable Implementation Specification: Protection From Malicious Software** Company has procedures for guarding against, detecting, and reporting malicious software.	Cloud Vendor: 0% Customer: 100%	N/A	The customer is responsible for developing anti-malware policies and procedures training customer workforce members regarding those policies and procedures.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
18	**§164.308(a)(5)(ii)(C)**	**Addressable Implementation Specification: Log-In Monitoring** Company has created procedures for monitoring log-in attempts and reporting discrepancies.	Cloud Vendor: 0% Customer: 100%	Cloud Vendors are responsible only for monitoring the areas of the environment for which they provide direct support. Cloud Vendors may provide access to some logging data for the customer's systems. Customers are responsible for monitoring all application/client level access to their databases to prevent unauthorized access including malicious/accidental changes or deletion of data.	The customer is responsible for log management and review activities, including log-in monitoring and reporting activities for any technical or physical environments containing PHI, including the cloud environment.
19	**§164.308(a)(5)(ii)(D)**	**Addressable Implementation Specification: Password Management** Company has created procedures for creating, changing, and safeguarding passwords.	Cloud Vendor: 0% Customer: 100%	N/A	The customer is responsible for creating password management policies and procedures, and providing password management training for the customer workforce members.
20	**§164.308(a)(6)(i)**	**Required Standard: Security Incident Procedures** Company has implemented policies and procedures to address security incidents.	Cloud Vendor: 0% Customer: 100%	Cloud Vendor does not monitor for security breaches or other security incidents within customers' applications or virtual machines. Customers are responsible for implementing appropriate monitoring in these and other systems they control. Cloud Vendors are responsible only for monitoring the areas of the environment for which they provide direct support.	The customer is responsible for security incident response activities for the customer cloud environment, as well as business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
21	**§164.308(a)(6)(ii)**	**Required Implementation Specification: Response and Reporting** Company identifies and responds to suspected or known security incidents; mitigates, to the extent practicable, harmful effects of security incidents that are known to Company; and documents security incidents and their outcomes.	Cloud Vendor: 10% Customer: 90%	Upon becoming aware of a Security Incident involving customer data, including PHI, a Cloud Vendor should have documented processes to report the Security Incident to the administrator(s) of the affected customer environments. Incidents should be reported to the customer within a contractually defined period of time.	The customer is responsible for security incident reporting activities for the customer cloud environment, as well as business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI. The customer is responsible for any breach notification activities to customers, law enforcement agencies, or other official notifications.
22	**§164.308(a)(7)(i)**	**Required Standard: Contingency Plan** Company has established and implemented policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.	Cloud Vendor: 60% Customer: 40%	Customer data can be stored in a redundant environment with robust backup, restore, and failover capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are generally used, ranging from redundant disks to guard against local disk failure to continuous, full data replication to a geographically dispersed datacenter.	The customer is responsible for developing business continuity plans to assure operational resilience in the customer's cloud environment, including provisions for assuring security controls remain in effect should the plan be implemented, in additions to plans for assuring the continuity of business processes in the event of a disaster.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
23	**§164.308(a)(7)(ii)(A)**	**Required Implementation Specification: Data Backup Plan** Company has established and implemented procedures to create and maintain retrievable exact copies of EPHI.	Cloud Vendor: 50% Customer: 50%	The Cloud Vendor has the ability to store multiple copies of data in different risk areas, and should be configured to replicate data to a backup data center (the geo-replication feature should be able to be disabled if desired).	The customer is responsible for ensuring backup policies and procedures have been developed and are implemented for the customer's cloud environment, and any other technical or physical environments containing PHI.
24	**§164.308(a)(7)(ii)(B)**	**Required Implementation Specification: Disaster Recovery Plan** Company has established and implemented procedures to restore any loss of data.	Cloud Vendor: 60% Customer: 40%	Customer data can be stored in a redundant environment with robust backup, restore, and failover capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are generally used, ranging from redundant disks to guard against local disk failure to continuous, full data replication to a geographically dispersed datacenter.	The customer is responsible for developing disaster recovery policies and procedures to enable to enable availability, business continuity, and rapid recovery for the customer's cloud environment, including provisions for assuring security controls remain in effect should the plan be implemented, in additions to plans for assuring the ability to recover business processes in the event of a disaster.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
25	**§164.308(a)(7)(ii) (C)**	**Required Implementation Specification: Emergency Mode Operation Plan** Company has established and implemented procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.	Cloud Vendor: 25% Customer: 75%	Customer data can be stored in a redundant environment with robust backup, restore, and failover capabilities to enable availability, business continuity, and rapid recovery. Multiple levels of data redundancy are generally used, ranging from redundant disks to guard against local disk failure to continuous, full data replication to a geographically dispersed datacenter.	The customer is responsible for developing business continuity plans to assure operational resilience in the customer's cloud environment, including provisions for assuring security controls remain in effect should the plan be implemented, in additions to plans for assuring the continuity of business processes in the event of a disaster.
26	**§164.308(a)(7)(ii) (D)**	**Addressable Implementation Specification: Testing and Revision Procedures** Company has implemented procedures for periodic testing and revision of contingency plans.	Cloud Vendor: 40% Customer: 60%	Third party audit documents should provide evidence that recovery plans are validated on a regular basis per industry best practices to ensure that solutions are viable at time of event.	The customer is responsible for testing business continuity plans for their cloud environment and business processes in the event of a disaster.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
27	**§164.308(a)(7)(ii)(E)**	**Addressable Implementation Specification: Applications and Data Criticality Analysis** Company has assessed the relative criticality of specific applications and data in support of other contingency plan components.	Cloud Vendor: 0% Customer: 100%	Customers are responsible for their environment after their cloud service has been provisioned. This responsibility includes applications, data content, virtual machines, access credentials, and compliance with regulatory requirements applicable to a particular industry and/or location.	The customer is responsible for defining the security and regulatory classifications of any data and objects within the business, including data in the cloud environment. The customer is responsible for identifying the criticality of systems to support their business continuity and disaster recovery plans.
28	**§164.308(a)(8)**	**Required Standard: Evaluation** Company has performed a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the Security Standards, and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which Company's security policies and procedures meet the requirements of the Security	Cloud Vendor: 30% Customer: 70%	The Cloud Vendor should undergo an annual third-party audit by internationally recognized auditors to provide independent attestation of compliance with published policies and procedures for security, privacy, continuity and compliance. The audits should include standard audit frameworks such as SSAE 16 and/or ISO 27001 to verify that the controls are effective and that the management system is appropriate.	The customer is responsible for performing periodic evaluations of the cloud computing environment at least annually to meet HIPAA requirements. In addition to these annual evaluations, the customer should perform regular vulnerability assessments and an annual penetration test of the customer's cloud environment, as well as any on premise environments.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
		Standards.			
29	**§164.306(e)**	**Required Maintenance:** Company reviews and modifies the security measures it has implemented in compliance with the Security Standards as needed to continue provision of reasonable and appropriate protection of EPHI, and updates documentation of such security measures.	Cloud Vendor: 0% Customer: 100%	Customers are responsible for determining if their Cloud Vendor's services can be compliant with their regulatory requirements based on the particular applications they intend to run in the cloud. Each customer must implement the required compliance mechanisms, policies, and procedures and is responsible for ensuring they do not violate regulatory requirements when using the cloud.	The customer is responsible for performing continuous monitoring of the customer's environment, including the cloud environment, for such things as configuration changes, data backup, and perimeter monitoring, to quickly identify potential changes in security operations.
30	**§164.308(b)(1)–(2)**	**Permissible Business Associate Contracts and Other Arrangements:** Company may permit a Business Associate to create, receive, maintain, or transmit EPHI on Company's behalf only if Company obtains satisfactory assurances that Business Associate will appropriately safeguard the information.	Cloud Vendor: 20% Customer: 80%	The Cloud Vendor must offer a BAA to customers wishing to use the service for applications that may access, create, transmit, or store ePHI. The customer is responsible for determining if the BAA offered by the Cloud Vendor meets legal and customer requirements.	The customer is responsible for obtaining BAAs with any third parties, including the cloud provider, who have access to data or for any technical or physical environments containing PHI.

		Company is not required to obtain such satisfactory assurances from a Business Associate that is a subcontractor. A Business Associate may permit a Subcontractor Business Associate to create, maintain, or transmit EPHI on its behalf only if it obtains satisfactory assurances that subcontractor will safeguard the EPHI appropriately.			
31	**§164.308(b)(3)**	**Required Implementation Specification: Written Contract or Other Arrangement** Company has documented the satisfactory assurances required by the Security Standards through a written contract or other arrangement with Business Associate.	Cloud Vendor: 20% Customer: 80%	The Cloud Vendor must offer a BAA to customers wishing to use the service for applications that may access, create, transmit, or store ePHI. The customer is responsible for determining if the BAA offered by the Cloud Vendor meets legal and customer requirements.	The customer is responsible for obtaining BAAs with any third parties, including the cloud provider, who have access to data or for any technical or physical environments containing PHI.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
32	**§164.316(a)**	**Required Standard: Policies and Procedures** Company has implemented reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Standards. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of the Security Standards. Company may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the Security Standards.	Cloud Vendor: 30% Customer: 70%	The Cloud Vendor should provide customers with their information security policies upon request. Customers and prospective customers may be required to sign a Non-Disclosure Agreement in order to receive a copy of the policies.	The customer is responsible for security policies and processes that includes administrative, physical, and technical controls to maintain compliance with applicable legal, statutory, and regulatory compliance obligations in the provision and maintenance of the customer's cloud environment, as well as the customer business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
33	**§164.316(b)(1)(i)–(ii)**	**Required Standard: Documentation** Company maintains the policies and procedures implemented to comply with the Security Standards in written (which may be electronic) form; and if an action, activity or assessment is required by the Security Standards to be documented, Company maintains a written (which may be electronic) record of the action, activity, or assessment.	Cloud Vendor: 33% Customer: 67%	Third party audit documents should provide evidence that the Cloud Vendor follows a common security framework and maintains documentation as required by that framework.	The customer is responsible for maintaining the security policies and processes documentation for the customer's cloud environment, as well as the customer business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI.
34	**§164.316(b)(2)(i)**	**Required Implementation Specification: Time Limit** Company retains the documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Cloud Vendor: 0% Customer: 100%	Third party audit documents should provide evidence that all security program documentation is retained for the appropriate period of time.	The customer is responsible for retention of the security policies and processes documentation for the customer's cloud environment, as well as the customer business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
35	**§164.316(b)(2)(ii)**	**Required Implementation Specification: Availability** Company makes documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Cloud Vendor: 50% Customer: 50%	The Cloud Vendor should provide customers with their information security policies upon request. Customers and prospective customers may be required to sign a Non-Disclosure Agreement in order to receive a copy of the policies. Third party audit documents should provide evidence that the Cloud Vendor follows a common security framework and maintains documentation as required by that framework.	The customer is responsible for the availability of the customer security policies and processes in the customer's cloud environment, as well as the customer business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI.
36	**§164.316(b)(2)(iii)**	**Required Implementation Specification: Updates** Company reviews documentation periodically, and updates as needed, in response to environmental or operational changes affecting the security of the EPHI.	Cloud Vendor: 33% Customer: 67%	Third party audit documents should provide evidence that the Cloud Vendor information security policies undergo a formal review and update process at a regularly scheduled interval not to exceed one year.	The customer is responsible for the regular review and update of the customer security policies and processes for the customer's cloud environment, as well as the customer business functions that require access to, creation or modification of, or transmission and storage of PHI in the cloud, and any other technical or physical environments containing PHI. .
PHYSICAL SAFEGUARDS					
37	**§164.310(a)(1)**	**Required Standard: Facility Access Controls** Company has implemented policies and procedures to	Cloud Vendor: 70% Customer: 30%	Third party audit documents should provide evidence that the Cloud Vendor has appropriate controls and systems in place to monitor access to the	The customer is responsible for security access to the systems in customer facilities.

		limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.		systems and physical hardware within the datacenters, and that all such access is tightly controlled and managed.	
38	**§164.310(a)(2)(i)**	**Addressable Implementation Specification: Contingency Operations** Company has established and implemented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Cloud Vendor: 50% Customer: 50%	Third party audit documents should provide evidence that a process for contingency operations is tested and functioning for the Cloud Vendor environment. This process should replicate the security, compliance and privacy requirements of the production environment at the alternate site.	The customer is responsible for developing contingency plans to assure operational resilience in the customer's cloud environment, including provisions for assuring security controls remain in effect should the plan be implemented, in additions to plans for assuring the continuity of business processes in the event of a disaster.
39		**Addressable Implementation Specification: Facility Security Plan** Company has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Cloud Vendor: 70% Customer: 30%	Third party audit documents should provide evidence that the Cloud Vendor has appropriate controls and systems in place to monitor access to the systems and physical hardware within the datacenters, and that all such access is tightly controlled and managed.	The customer is responsible for security access to the systems in customer facilities.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
40	**§164.310(a)(2)(iii)**	**Addressable Implementation Specification: Access Control and Validation Procedures** Company has implemented procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Cloud Vendor: 50% Customer: 50%	Third party audit documents should provide evidence that the Cloud Vendor has appropriate controls and systems in place to monitor access to the systems and physical hardware within the datacenters, and that all such access is tightly controlled and managed.	The customer is responsible for security access to the systems in customer facilities.
41	**§164.310(a)(2)(iv)**	**Addressable Implementation Specification: Maintenance Records** Company has implemented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (*e.g.,* hardware, walls, doors, and locks).	Cloud Vendor: 50% Customer: 50%	Third party audit documents should provide evidence that the Cloud Vendor has appropriate controls and systems in place to identify and document repairs to the systems and physical hardware within the datacenter.	The customer is responsible for documenting repairs and modifications to the security controls in customer facilities.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
42	**§164.310(b)**	**Required Standard: Workstation Use** Company has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.	Cloud Vendor: 0% Customer 100%	The Cloud Vendor is responsible for the infrastructure platforms, including whether they offer services that can be configured to meet the security, privacy, and compliance needs of most customers. However, customers are responsible for their environment after their cloud service has been provisioned. This responsibility includes applications, data content, virtual machines, workstations, access credentials, and compliance with regulatory requirements applicable to a particular industry and/or location.	The customer is responsible for workstation use policies for the customer business functions that require access to, creation or modification of, or transmission and storage of storage of PHI in the cloud, and any other technical or physical environments containing PHI.
43	**§164.310(c)**	**Required Standard: Workstation Security** Company has implemented physical safeguards for all workstations that access EPHI, to restrict access to authorized users.	Cloud Vendor: 0% Customer: 100%	The Cloud Vendor is responsible for the infrastructure platforms, including whether they offer services that can be configured to meet the security, privacy, and compliance needs of most customers. However, customers are responsible for their environment after their cloud service has been provisioned. This responsibility includes applications, data content, virtual machines, workstations, access credentials, and compliance with regulatory requirements applicable to a particular industry and/or location.	The customer is responsible for workstation safeguards for the customer business functions that require access to, creation or modification of, or transmission and storage of storage of PHI in the cloud, and any other technical or physical environments containing PHI.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
44	**§164.310(d)(1)**	**Required Standard: Device and Media Controls** Company has implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.	Cloud Vendor: 33% Customer: 67%	Third party audit documents should provide evidence that the Cloud Vendor has appropriate controls and systems in place to monitor access by removable media and wireless devices in datacenters, including alerts if removable media or devices are attached to systems.	The customer is responsible for device and media controls for the customer business functions that require access to, creation or modification of, or transmission and storage of storage of PHI in the cloud, and any other technical or physical environments containing PHI.
45	**§164.310(d)(2)(i)**	**Required Implementation Specification: Disposal** Company has implemented policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.	Cloud Vendor: 40% Customer: 60%	Third party audit documents should provide evidence that the Cloud Vendor uses best practice procedures and a wiping solution that is NIST 800-88 (National Institute of Standards & Technology Special Publication 800-88, Guidelines for Media Sanitization) compliant. For hard drives that can't be wiped that includes a physical destruction process that destroys them (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate).	The customer is responsible for media disposal procedures for all customer owned media.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
46	**§164.310(d)(2)(ii)**	**Required Implementation Specification: Media Re-Use** Company has implemented procedures for removal of EPHI from electronic media before the media are made available for re-use.	Cloud Vendor: 40% Customer: 60%	Third party audit documents should provide evidence that the Cloud Vendor uses best practice procedures and a wiping solution that is NIST 800-88 (National Institute of Standards & Technology Special Publication 800-88, Guidelines for Media Sanitization) compliant. For hard drives that can't be wiped that includes a physical destruction process that destroys them (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate).	The customer is responsible for media reuse procedures for all customer owned media.
47	**§164.310(d)(2)(iii)**	**Addressable Implementation Specification: Accountability** Company maintains a record of the movement of hardware and electronic media and any person responsible for such hardware and electronic media.	Cloud Vendor: 0% Customer: 100%	The Cloud Vendor does not monitor the applications and data that customers choose to run in Cloud Vendor and thus will not know when hardware or electronic media contains ePHI.	The customer is responsible for device and media controls for the customer business functions that require access to, creation or modification of, or transmission and storage of storage of PHI in the cloud, and any other technical or physical environments containing PHI.
48	**§164.310(d)(2)(iv)**	**Addressable Implementation Specification: Data Backup and Storage** Company creates a retrievable, exact copy of EPHI, when needed, before movement of equipment.	Cloud Vendor: 45% Customer: 55%	The Cloud Vendor has the ability to store multiple copies of data in different risk areas, and should be configured to replicate data to a backup data center (the geo-replication feature should be able to be disabled if desired).	The customer is responsible for implementing the desired backup plans for any technical or physical environments containing storage of PHI in the cloud, and any other technical or physical environments containing PHI.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
TECHNICAL SAFEGUARDS					
49	**§164.312(a)(1)**	**Required Standard: Access Control** Company has implemented technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights.	Cloud Vendor: 45% Customer: 55%	Third party audit documents should provide evidence that access control for the Cloud Vendor employees is provided using role-based access and follow the principle of least privilege for access to all vendor environments.	The customer is responsible for authorizing and providing all access to systems and data within the customer's cloud environment, including configuring role-based access that provides minimum necessary levels of access rights. If multi-factor authentication is desired, the customer is responsible for identifying and implementing the appropriate MFA tools.
50	**§164.312(a)(2)(i)**	**Required Implementation Specification: Unique User Identification** Company assigns a unique name and/or number for identifying and tracking user identity.	Cloud Vendor: 35% Customer: 65%	Third party audit documents should provide evidence that access to data is traceable to a unique user.	The customer is responsible for authorizing and providing all access to systems and data within the customer's cloud environment, including configuring role-based access that provides minimum necessary levels of access rights. If multi-factor authentication is desired, the customer is responsible for identifying and implementing the appropriate MFA tools.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
51	**§164.312(a)(2)(ii)**	**Required Implementation Specification: Emergency Access Procedure** Company has established and implemented procedures for obtaining necessary EPHI during an emergency.	Cloud Vendor: 50% Customer: 50%	Third party audit documents should provide evidence that a process for contingency operations is tested and functioning for the Cloud Vendor environment. This process should replicate the security, compliance and privacy requirements of the production environment at the alternate site.	The customer is responsible for developing contingency plans to assure operational resilience and access to data in the customer's cloud environment, including provisions for assuring security controls remain in effect should the plan be implemented, in additions to plans for assuring the continuity of business processes in the event of a disaster.
52	**§164.312(a)(2)(iii)**	**Addressable Implementation Specification: Automatic Logoff** Company has implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Cloud Vendor: 0% Customer: 100%	Customers are responsible for their environment after their cloud service has been provisioned. This responsibility includes applications, data content, virtual machines, access credentials, and compliance with regulatory requirements applicable to a particular industry and/or location.	The customer is responsible for workstation and application safeguards for the customer business functions that require access to, creation or modification of, or transmission and storage of storage of PHI in the cloud, and any other technical or physical environments containing PHI.
53	**§164.312(a)(2)(iv)**	**Addressable Implementation Specification: Encryption and Decryption** Company has implemented a mechanism to encrypt and decrypt EPHI.	Cloud Vendor: 0% Customer: 100%	Cloud Vendors typically do not automatically encrypt customer data at rest. Customers are usually responsible for implementing encryption at rest using additional cryptographic services.	The customer is responsible for encryption, including encryption key management processes, for PHI stored in customer cloud environments as well as all customer owned systems, technical or physical environments containing PHI.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Customer Security Controls
54	**§164.312(b)**	**Required Standard: Audit Controls** Company has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.	Cloud Vendor: 10% Customer: 90%	Cloud Vendors are responsible only for monitoring the areas of the environment for which they provide direct support. Cloud Vendors may provide access to some logging data for the customer's systems. Customers are responsible for monitoring all application/client level access to their databases to prevent unauthorized access including malicious/accidental changes or deletion of data.	The customer is responsible for collecting and monitoring logs from all systems supported within the customer's cloud environment, including customer's application-specific logs. Potential issues must be identified, tracked, and resolved.
55	**§164.312(c)(1)**	**Required Standard: Integrity** Company has implemented policies and procedures to protect EPHI from improper alteration or destruction.	Cloud Vendor: 0% Customer: 100%	Cloud Vendor customers are responsible for ensuring the integrity of the information that's written to storage by their applications. For example, customers are responsible for monitoring all application/client level access to their databases to prevent unauthorized access including malicious/accidental changes or deletion of data.	The customer is responsible for collecting and monitoring logs from all systems supported within the customer's cloud environment, including customer's application-specific logs. Potential issues must be identified, tracked, and resolved. The customer is responsible for all application-specific security controls that maintain integrity.
56	**§164.312(c)(2)**	**Addressable Implementation Specification: Mechanism to Authenticate**	Cloud Vendor: 0% Customer: 100%	Cloud Vendor customers are responsible for ensuring the integrity of the information that's written to storage by	The customer is responsible for collecting and monitoring logs from all systems supported within the customer's cloud

		EPHI Company has implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.		their applications. For example, customers are responsible for monitoring all application/client level access to their databases to prevent unauthorized access including malicious/accidental changes or deletion of data.	environment, including customer's application-specific logs. Potential issues must be identified, tracked, and resolved. The customer is responsible for all application-specific security controls that maintain integrity.
57	**§164.312(d)**	**Required Standard: Person or Entity Authentication** Company has implemented procedures to verify that a person or entity seeking access to EPHI is the one claimed.	Cloud Vendor: 30% Customer: 70%	Third party audit documents should provide evidence that the Cloud Vendor uses secure two-factor authentication for remote access, and uses sufficiently complex controls for on-site access to properly authenticate users.	The customer is responsible for person or entity authentication for all access to systems and data within the customer's cloud environment, and any other technical or physical environments containing PHI.
58	**§164.312(e)(1)**	**Required Standard: Transmission Security** Company has implemented technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.	Cloud Vendor: 0% Customer: 100%	Customers are usually responsible for implementing encryption in transit using additional cryptographic services.	The customer is responsible for transmission security for any technical or physical environments containing PHI, including cloud environments.
59	**§164.312(e)(2)(i)**	**Addressable Implementation Specification: Integrity Controls** Company has implemented security measures to ensure that	Cloud Vendor: 0% Customer: 100%	Customers are usually responsible for implementing encryption in transit using additional cryptographic services.	The customer is responsible for transmission security for any technical or physical environments containing PHI, including cloud environments.

		electronically transmitted EPHI is not improperly modified without detection until disposed of.			
60	**§164.312(e)(2)(ii)**	**Addressable Implementation Specification: Encryption** Company has implemented a mechanism to encrypt EPHI whenever deemed appropriate.	Cloud Vendor: 0% Customer: 100%	The Cloud Vendor will not monitor the applications and data that customers choose to run in Cloud Vendor, thus does not know where ePHI may reside. Customers are usually responsible for implementing encryption in transit using additional cryptographic services.	The customer is responsible for appropriate encryption for any technical or physical environments containing PHI, including cloud environments.

The data shown here does not reflect a specific cloud provider, as noted before, but it represents a fairly typical public cloud environment that a customer will find as they consider the out of the box offerings from a public cloud provider. Customers must be clear on what services are provided by the cloud vendor and what remains a customer responsibility. They then have to ensure that this remaining portion is addressed as well. The missing components can be provided by the customer themselves, or they can be provided in collaboration with a service provider that can assist and facilitate much of this gap in such a way that all the HIPAA requirements are met and can be validated for auditors.

Once a company moves systems or data off their own premises into a cloud environment, the compliance effort must be a collaboration between the entities. The cloud vendor in and of themselves cannot provide full compliance, and neither can the customer. It is the sum of the parts that make the whole. Compliance is not a statement but rather a process, and all parties must have the appropriate processes implemented and continuously managed. The good news is that customers can assemble the necessary controls and processes to be able to take full advantage of the benefits the cloud has to offer and be able to do it while having a high level of security and meeting the HIPAA regulatory requirements.

Lumen21 is a company that specializes in the area of IT Security and Compliance. Lumen21 has a number of solutions and services for healthcare organizations to use to take advantage of the newest technology while meeting their regulatory and safety responsibilities. Lumen21's compliant cloud computing solution is truly HIPAA compliant. The Lumen21 solution is compliant with FFIEC, HIPAA/HITECH, PCI and FISMA requirements. The Lumen21-compliant cloud computing solution also complies with NIST SP-800-144, NIST SP 500-299 standards and meets or exceeds the Cloud Security Alliance Framework (CSA). Lumen21 enables the compliance process and allows a healthcare company the ability to measure, monitor, report and improve that process. Lumen21 offers its O365+ compliance service by 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's why at Lumen21 we believe that HIPAA compliance is not a statement, it's an ongoing vetted and certified process.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