Lumen21

Compliant Cloud Computing Solution

Lumen21

As explained in HIPAA Compliance in the Cloud: Addressing the Gaps, highly regulated companies, such as healthcare, have many concerns and responsibilities as a user of cloud technology. There are things that are facilitated by cloud vendors, but they only go so far, leaving the consumer to address the HIPAA and security requirements of given application workloads that are moved into the cloud.

A company moving workloads to the cloud can dedicate time, effort, expertise and monies to assembling the added components that are required for the regulations that a healthcare organization will need to comply with and to which they must attest. While that may seem more feasible for larger healthcare organizations with dedicated compliance, security and IT teams, even larger organizations have numerous projects they are dealing with and are challenged by resource constraints. Smaller organizations may not have the expertise and or resources to be able to assemble the needed environment. This dilemma contributes to the lower cloud adoption rates within healthcare organizations.

These companies can, however, turn to a provider that has devoted the time, effort and expertise to assemble the components that will help drive the security and compliance efforts beyond what the cloud provider provides. Lumen21 and its Compliant Cloud Computing environment provides such a solution to healthcare organizations. The Lumen21 Compliant Cloud can leverage either Microsoft Azure and or Amazon AWS cloud environments. Lumen21 provides a private cloud offering for a given client and within that cloud will apply the required security controls and compliance processes to ensure the compliance and security needs for each client, not only at the cloud level but also at the application level, are addressed. The solution, delivered as a service, provides that added level that helps fill the compliance gap.

Lumen21 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. We like to think we help drive compliance.

It is important to note that by leveraging a solution like the Lumen21 Compliant Cloud, a company will end up with a Compliance Framework for their cloud environment. Take for example how it works with Microsoft Azure:

Compliance Frameworks

Compliance certifications

Cloud Provider and Lumen21 maintain experts focused on ensuring that and the Lumen21 service meets Its own compliance obligations, which helps customers meet their own compliance requirements.

Continual evaluation, benchmarking adoption, test & audit

Compliance strategy helps customers address business objectives and industry standards & regulations, including ongoing evaluation and adoption of emerging standards and practices.

Independent verification

Microsoft Azure and Lumen21 C3 Compliant Cloud support ongoing verification by third-party audit firms.

Access to audit reports

Microsoft and Lumen21 share audit report findings and compliance packages with customers.

Best practices

Prescriptive guidance on securing data, apps. and infrastructure in Azure makes it easier for customers to achieve compliance.

Compliance monitoring and reporting

Lumen21 C3 Compliant Cloud service provides ongoing management, security monitoring and compliance processes and reporting of the customer's individual Azure cloud environment.

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 cannotprovide full compliance, and neither can the customer or service provider like Lumen21. However, as shown in the Matrix above, it is the sum of the parts that make the whole. All parties must have the appropriate processes implemented and continuously managed in order to be able to achieve the needed compliance and do so while not sacrificing security.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 80% Customer: 20%	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.	Lumen21 provides customer-specific environments within a Cloud Vendor that have been designed to meet HIPAA and HITECH Physical and Technical Safeguards. In addition, all services provided by Lumen21 for Compliant Cloud Computing customers are performed to meet the HIPAA and HITECH Administrative Safeguards. Lumen21 and the Compliant Cloud Computing environment have been evaluated by a third party and comply with the Common Security Framework.	The customer is responsible for providing security policies and procedures for customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 70% Customer: 10%	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 Lumen21-supported cloud computing environment, including all managed customer services and systems within the cloud, undergoes annual evaluation.	The customer is responsible for performing risk assessment activities for customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
3	**§164.308(a)(1)(ii)(B), §164.306(a)**	**Required Implementation Specification: Risk Analysis** Company has	Cloud Vendor: 0% Lumen21: 90% Customer: 10%	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	Lumen21 has implemented the Common Security Framework controls in the	The customer is responsible for implementing any required security measures for customer business

		implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.		sufficient to reduce potential risks and vulnerabilities to a reasonable and appropriate level.	Compliant Cloud Computing environment for each customer with which it has a signed BAA.	functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 34% Customer: 33%	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.	All Lumen21 employees agree to abide by a documented Code of Conduct that includes a formal discipline process and potential sanctions for violations, including violations of any Information Security Policies.	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% Lumen21: 85% Customer: 5%	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.	Lumen21 provides 24x7x365 eyes-on-screen monitoring of all systems supported within the Compliant Cloud Computing environment, including collecting and monitoring data from the Windows Cloud Vendor Diagnostics. Potential issues are identified and escalated to the Lumen21 Network Operations Center for attention and resolution.	The customer is responsible for informing Lumen21 of any application-specific logs that should be monitored.
6	**§164.308(a)(2)**	**Required Standard: Assigned Security**	Cloud Vendor: 33% Lumen21: 34% Customer: 33%	Third party audit documents should provide evidence of management commitment to information security and	The Lumen21 Compliant Cloud Computing environment was	The customer is responsible for assigning security responsibility with

		Responsibility Company has identified the security official who is responsible for the development and implementation of the security policies and procedures of Company.		management responsibility.	developed specifically to meet the needs of organizations with specific security and regulatory compliance requirements, such as healthcare entities, financial services companies, banks, credit unions, retail stores, utilities, online retailers, restaurants and government agencies. As a result, a Lumen21 executive has been identified as responsible for maintaining a robust Information Security Management Program. Information security policies are reviewed and approved by executive management, and are reviewed at least annually. Policies and procedures documents include assigning responsibility for policy enforcement.	the company for business functions.
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% Lumen21: 75% Customer: 20%	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.	Lumen21 may perform access administration functions as part of cloud management services if covered within the contract, however access will be granted only with documented approval of the customer. Users are limited to specific defined, documented and approved applications and minimum necessary levels of access rights. Multi-Factor Authentication is provided for all remote access as a standard for	The customer is responsible for authorizing all access to customer data within the Compliant Cloud Computing environment.

					Lumen21 Compliant Cloud Computing Environment.	
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% Lumen21: 34% Customer: 33%	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.	All individuals granted access to Lumen21 information assets must be authorized by appropriate management. Lumen21 provides supervision of Lumen21 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% Lumen21: 34% Customer: 33%	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.	As a condition of employment, all employees, in all employment categories and classifications, must receive a grade of PASS on our comprehensive standard verifications and background screening process. The background check includes, but is not limited to, verification of identity, criminal screening, employment and education verification, and drug testing.	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	Cloud Vendor: 33% Lumen21: 34% Customer: 33%	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.	Lumen21 uses a comprehensive exit checklists that includes IT notification for elimination of access within 24 hours upon employee termination.	The customer is responsible for termination policies and procedures for customer workforce members.

		member ends or as otherwise determined by Company.				
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% Lumen21: 75% Customer: 20%	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.	Lumen21 may perform access administration functions as part of cloud management services if covered within the contract, however access will be granted only with documented approval of the customer. Users are limited to specific defined, documented and approved applications and minimum necessary levels of access rights. Multi-Factor Authentication is provided for all remote access as a standard for Lumen21 Compliant Cloud Computing Environment.	The customer is responsible for authorizing all access to customer data within the Compliant Cloud Computing environment.
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% Lumen21: 80% Customer: 10%	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 Lumen21 Compliant Cloud Computing network uses a segmented network with access control lists to provide physical separation of system interfaces. Clearinghouse environments are segregated from the larger organization using physical and/or logical separation that includes, at minimum, segregated network segments and virtual machines.	The customer is responsible for identifying any clearinghouse functions that must be segmented within the Compliant Cloud Computing environment.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 60% Customer: 10%	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.	All individuals granted access to Lumen21 information assets must be authorized by appropriate management. Users, including third party service providers, are limited to specific defined, documented and approved applications and minimum necessary levels of access rights.	The customer is responsible for authorization of all customer workforce members and any access granted to third parties, including Lumen21.
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% Lumen21: 60% Customer: 10%	Third party audit documents should provide evidence that access to Cloud Vendor assets is granted based upon management authorization.	All individuals granted access to Lumen21 information assets must be authorized by appropriate management. Users, including third party service providers, are limited to specific defined, documented and approved applications and minimum necessary levels of access rights. Managers or owners of applications and data are responsible for reviewing who has access on a periodic basis, including the granting, revoking, and review of user access rights. Regular access review audits occur to validate appropriate access provisioning has occurred.	The customer is responsible for authorization and review of all customer workforce members and any access granted to third parties, including Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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: 33% Lumen21: 34% Customer: 33%	Third party audit documents should provide evidence that all appropriate Cloud Vendor employees take part in a required security-training program.	All Lumen21 employees and contractors must take new-hire security awareness training.	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: 33% Lumen21: 34% Customer: 33%	Third party audit documents should provide evidence that all appropriate Cloud Vendor employees are recipients of periodic security awareness updates when applicable.	Regular awareness updates are provided to all employees at least quarterly.	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% Lumen21: 67% Customer: 33%	N/A	Lumen21 supports an active security awareness program for all employees that includes anti-malware awareness training, including the security of mobile devices.	The customer is responsible for providing required security training, including anti-malware training, for the customer workforce members.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 100% Customer: 0%	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 Lumen21 Compliant Cloud Computing environment provides a robust log management and review service, including log-in monitoring and reporting, that includes near-real-time correlation, 24x7x365 analysis of security and network events by certified, expert analysts, and secure, redundant log archival.	The customer is responsible for log management activities for any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 67% Customer: 33%	N/A	Lumen21 supports an active security awareness program for all employees that includes password management training.	The customer is responsible for providing required security training, including 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% Lumen21: 80% Customer: 20%	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 Lumen21 Incident Response process includes identification, containment, eradication, recovery, and reporting steps to manage a security event. Security of the cloud environment and the data maintained there is the priority at each step and will take precedence over collection of evidence to support legal action when the two are in conflict. The final step in the Lumen21 Incident Response process includes documenting and reporting on the incident to allow senior	The customer is responsible for security incident response activities for customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

					management to understand the types of security incidents that occur and the costs associated with those incidents as part of a continuous improvement program to reduce the volume and/or cost.	
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% Lumen21: 70% Customer: 20%	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.	Lumen21 has a documented Breach Notification and Incident Response policy that establishes the business processes and personnel responsibilities for security incident identification, reporting, response, investigation, and, where a potential breach has occurred, customer notification. Lumen21 maintains contacts with law enforcement, regulatory entities, security assessment organizations, and industry groups to obtain advice as needed, and assist the customer in any interface with law enforcement when required. Roles and responsibilities for managing and maintaining these relationships are defined.	The customer is responsible for security incident reporting activities for customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21. The customer is responsible for any breach notification activities to customers, law enforcement agencies, or other official notifications.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 25% Customer: 15%	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.	Lumen21 has developed a comprehensive business continuity plan to assure operational resilience in providing support and management for the Lumen21 Compliant Cloud Computing environment. Responsibilities are assigned to specific individuals, and the plan includes provisions for assuring security controls remain in effect should be plan be implemented.	The customer is responsible for developing plans for assuring the continuity of their business processes in the event of a disaster.
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% Lumen21: 45% Customer: 5%	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).	Lumen21 maintains a comprehensive policy and process library to support IT governance and service management, including backup requirements.	The customer is responsible for backup plans for any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 35% Customer: 5%	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 Lumen21 Business Continuity Plan provides a roadmap for maintaining support and management for our customer's cloud computing environments.	The customer is responsible for disaster recovery processes and procedures to enable customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 60% Customer: 15%	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.	Lumen21 has developed a comprehensive business continuity plan to assure operational resilience in providing support and management for the Lumen21 Compliant Cloud Computing environment. Responsibilities are assigned to specific individuals, and the plan includes provisions for assuring security controls remain in effect should be plan be implemented.	The customer is responsible for developing plans for assuring the continuity of their business processes in the event of a disaster, including security processes.
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% Lumen21: 50% Customer: 10%	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.	Business continuity and security incident response plans are tested at least annually, and an Executive Summary of test results is available for customer review upon request.	The customer is responsible for testing business continuity plans for their business processes in the event of a disaster.
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% Lumen21: 50% Customer: 50%	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.	A customer Business Impact Assessment is an integral part of the customer contracting and implementation process. The business impact assessment is reviewed at appropriate intervals. The Lumen21 Compliant Cloud Computing environment is designed to protect data classified as non-public from unauthorized disclosure, modification, or fraudulent use. Such classification	The customer is responsible for defining the security and regulatory classifications of any data and objects as part of the onboarding process and any changes that may occur during the contract.

					is defined by the customer during the onboarding process.	
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 Standards.	Cloud Vendor: 30% Lumen21: 60% Customer: 10%	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 Lumen21-enabled cloud computing environment is audited at least annually to validate compliance with our security, privacy, continuity, and compliance policies and procedures.	The customer is responsible for periodic evaluations of the customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 90% Customer: 10%	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.	Lumen 21 performs continuous monitoring of the customer's cloud environment, including configuration changes and perimeter monitoring to quickly identify potential changes in security operations. Data backup reports are monitored to assure data backups are available for business resumption activities. User access reports will be provided to the customer at least quarterly to be validated for accuracy.	The customer is responsible for review and modification of the security controls for the customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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. Company is not required to obtain such satisfactory assurances from a	Cloud Vendor: 20% Lumen21: 70% Customer: 10%	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.	Offers a standard BAA to all Lumen21 Compliant Cloud Customers that covers all data and services maintained and supported by Lumen21. Lumen21 has a signed BAA with Cloud Vendor and all other subcontractors.	The customer is responsible for obtaining BAAs with any third parties who have access to data or for any technical or physical environments containing PHI that are not managed by Lumen21.

		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% Lumen21: 70% Customer: 10%	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.	Offers a standard BAA to all Lumen21 Compliant Cloud Customers that covers all data and services maintained and supported by Lumen21. Lumen21 has a signed BAA with Cloud Vendor and all other subcontractors.	The customer is responsible for obtaining BAAs with any third parties who have access to data or for any technical or physical environments containing PHI that are not managed by Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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: 20% Lumen21: 50% Customer: 30%	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.	Lumen21 has developed a comprehensive, standards-based information security management program that includes administrative, physical and technical controls to maintain compliance with legal, statutory and regulatory standards regulatory compliance obligations for all services in the provision and maintenance of the Compliant Cloud environment.	The customer is responsible for security policies and processes for the customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 34% Customer: 33%	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 business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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: 33% Lumen21: 34% Customer: 33%	Third party audit documents should provide evidence that all security program documentation is retained for the appropriate period of time.	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 business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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: 33% Lumen21: 34% Customer: 33%	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 Lumen21 Information Security Management Program is available to all relevant stakeholders.	The customer is responsible for the availability of the customer-specific security policies and processes.
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% Lumen21: 34% Customer: 33%	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.	Information security policies are reviewed and approved by executive management, and are reviewed and updated at least annually. Policies and procedures documents include assigning responsibility for policy enforcement.	The customer is responsible for the regular review and update of the customer-specific security policies and processes.
PHYSICAL SAFEGUARDS						
37	**§164.310(a)(1)**	**Required Standard: Facility Access Controls** Company has implemented policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that	Cloud Vendor: 70% Lumen21: 20% Customer: 10%	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.	Lumen21 facilities have appropriate controls in place to monitor access to the systems and to the Lumen21 physical facilities. Lumen21 uses an inventory and asset management program that tracks all organizationally-managed assets. The inventory is automatically updated on a defined schedule, including patch	The customer will define the security and regulatory classifications of any data and objects as part of the onboarding process, and logical data flow diagrams for all customer environments are created as part of the implementation process. The customer is responsible for security access to

		properly authorized access is allowed.			levels, applications installed, security software configurations, and asset owner.	the systems in customer facilities.
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% Lumen21: 40% Customer: 10%	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 Lumen21 Compliant Cloud Computing environment is supported by a continuity solution that reflects the security, compliance and privacy requirements of the service production environment at the alternate site. Systems will be replicated in at least two independent regions, allowing for continued service in the event of a regional outage. The continuity solution supports a quarterly uptime of 99.9% and includes redundancy at the physical, data, and functional layers, providing high availability and disaster recovery capabilities to keep customers up and running.	The customer is responsible for contingency operations for the customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 20% Customer: 10%	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.	Lumen21 facilities have appropriate controls in place to monitor access to the systems and to the Lumen21 physical facilities.	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	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 40% Customer: 10%	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.	Access to Lumen21 facilities is restricted. The main interior or reception areas have electronic card access control devices on the perimeter door(s), which restrict access to the interior facilities. Rooms within the facility that contain critical systems (servers, generators, electrical panels, network equipment, etc.) are restricted through various security mechanisms such as electronic card access, keyed lock, anti-tailgating and/or biometric devices. Front desk personnel are required to positively identify Full-Time Employees (FTEs) or authorized Contractors without ID cards. All guests are required to wear guest badges and be escorted by authorized Lumen21 personnel.	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	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 40% Customer: 10%	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.	Lumen21 maintains records of all modifications or repairs to the facility components related to security controls.	The customer is responsible for documenting repairs and modifications to the security controls in customer facilities.
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% Lumen21: 50% Customer: 50%	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.	Lumen21's Acceptable Use Policy defines the appropriate use of all Lumen21 assets including tangible property such as desks and computers, and intangible property such as information, ideas and electronic communications. The acceptable use policy specifically covers use of company property, use of personal property, proprietary and confidential information assets, electronic communications, and Internet and social media postings.	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 PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
43	**§164.310(c)**	**Required Standard: Workstation Security** Company has implemented physical safeguards for	Cloud Vendor: 0% Lumen21: 70% Customer: 30%	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,	Lumen21 has implemented technical controls that include session time-out and screen-locking, physical controls that limit unauthorized users	The customer is responsible for workstation safeguards for the customer business functions that require access to, creation or modification of, or

		all workstations that access EPHI, to restrict access to authorized users.		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.	from accessing facilities, and administrative policies that require employees to lock workstations and maintain a clean-desk policy. Where Lumen21 supports customer workstations or cloud-based remote desktops, these controls are included in the customer environment	transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 34% Customer: 33%	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.	Lumen21 uses an inventory and asset management program that tracks all organizationally-owned assets. Lumen21 has implemented removable media controls that can either prevent the use of removable media entirely, or allow only fully encrypted removable media, based on user privileges. No personal mobile devices are permitted to be used on the corporate network at any time. Corporate email on a smartphone is restricted to an encrypted container that is access-controlled and fully managed by Lumen21 administrators.	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 PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
45	**§164.310(d)(2)(i)**	**Required Implementation Specification: Disposal** Company has implemented	Cloud Vendor: 40% Lumen21: 50% Customer: 10%	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	Lumen21 has strict policies regarding the disposal of equipment that include using a Secure Erase process that meets	The customer is responsible for media disposal procedures for the customer owned media.

		policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.		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).	DoD 5220.22-M and NIST 800-88 requirements that make recovery of the information impossible.	
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% Lumen21: 50% Customer: 10%	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).	Lumen21 has strict policies regarding the disposal of equipment that include using a Secure Erase process that meets DoD 5220.22-M and NIST 800-88 requirements that make recovery of the information impossible.	The customer is responsible for media reuse procedures for the 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% Lumen21: 50% Customer: 50%	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.	Lumen21's mobile device management process includes administrative, physical, and technical controls to manage the risks associated with mobile devices, including asset management for all corporate-owned mobile devices and removable media controls that can either prevent the use of removable media entirely, or allow only fully encrypted removable media, based on user privileges. No personal mobile devices are permitted to be used on the corporate network at any time. Use of personal smartphones to access corporate email is available with management approval.	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 PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

					Corporate email on a smartphone is restricted to an encrypted container that is access-controlled and fully managed by Lumen21 administrators.	
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% Lumen21: 50% Customer: 5%	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).	Lumen21 maintains a comprehensive library of policies and processes to support IT governance and service management, including supporting requirements.	The customer is responsible for backup plans for any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 45% Customer: 10%	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.	Lumen21 uses Active Directory to store and manage identify information and grant access privileges. Users are limited to specific defined, documented and approved applications and levels of access rights. Computer and communication system access control is achieved via user IDs that are unique to each individual user to provide individual accountability. Users are limited to specific defined, documented and approved applications and minimum necessary levels of access rights. Lumen21 policy requires evaluating segregation of duties controls to prevent fraud or error when approving access rights.	The customer is responsible for access controls for the customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 55% Customer: 10%	Third party audit documents should provide evidence that access to data is traceable to a unique user.	Access control is achieved via user IDs that are unique to each individual user to provide individual accountability.	The customer is responsible for access controls for the customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 40% Customer: 10%	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 Lumen21 Compliant Cloud Computing environment is supported by a continuity solution that reflects the security, compliance and privacy requirements of the service production environment at the alternate site. Systems will be replicated in at least two independent regions, allowing for continued service in the event of a regional outage. The continuity solution supports a quarterly uptime of 99.9% and includes redundancy at the physical, data, and functional layers, providing high availability and disaster recovery capabilities to keep customers up and running.	The customer is responsible for contingency operations for the customer business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
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% Lumen21: 70% Customer: 30%	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.	Lumen21 has implemented technical controls that include session time-out and screen-locking, physical controls that limit unauthorized users from accessing facilities, and administrative policies that require employees to lock workstations and maintain a clean-desk policy. Where Lumen21 supports customer workstations or cloud-based remote desktops, these controls are included in the customer environment	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 PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 80% Customer: 20%	Cloud Vendors typically do not automatically encrypt customer data at rest. Customers are usually responsible for implementing encryption at rest using additional cryptographic services.	All Storage will be Encrypted and the keys will be stored in Authentication Systems or Third Party Key Management Software. All encryption keys will be owned by the data owner, and key management responsibilities will be identified during implementation.	The customer is responsible for encryption for customer owned systems containing ePHI, and any technical or physical environments containing PHI that are not managed by Lumen21.

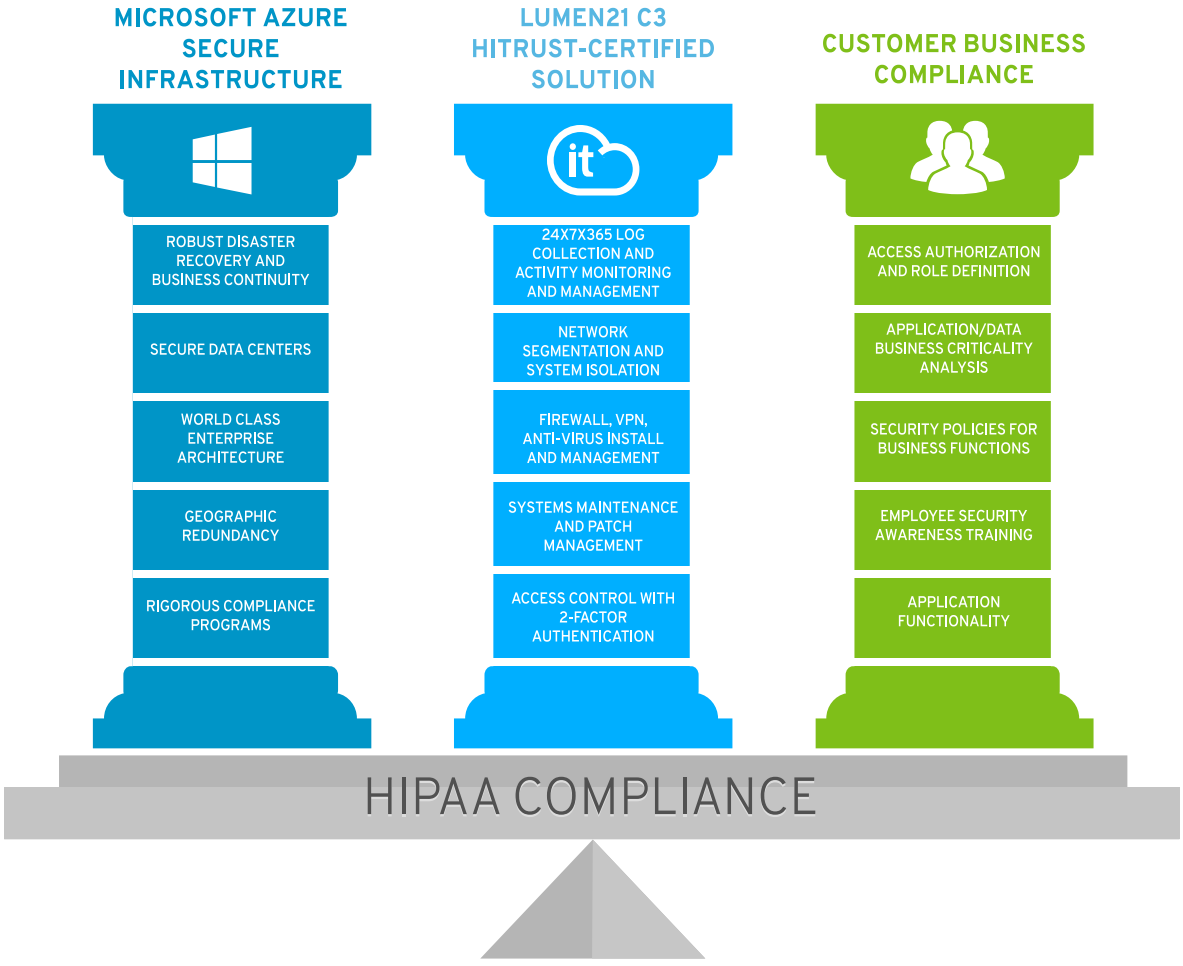
#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
54	**§164.312(b)**	**Required Standard: Audit Controls** Company has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.	Cloud Vendor: 10% Lumen21: 85% Customer: 5%	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.	Lumen21 provides 24x7x365 eyes-on-screen monitoring of all systems supported within the Compliant Cloud Computing environment, including collecting and monitoring data from the Windows Cloud Vendor Diagnostics. Potential issues are identified and escalated to the Lumen21 Network Operations Center for attention and resolution. Data backup reports are monitored to assure data backups are available for business resumption activities. User access reports will be provided at least quarterly to be validated for accuracy.	The customer is responsible for informing Lumen21 of any application-specific logs that should be monitored.
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% Lumen21: 85% Customer: 15%	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.	Lumen21 performs continuous monitoring of the customer's cloud environment, including configuration changes and perimeter monitoring to quickly identify potential changes in security operations. Any security, contractual, and regulatory requirements for data exchange are defined and documented as part of the onboarding process and	The Lumen21 Compliant Cloud Computing environment provides infrastructure services. Application-specific security controls are the responsibility of the customer and the application developer. The customer is responsible for informing Lumen21 of any application-specific logs that should be monitored.

					included in the implementation plans. Lumen21 will assist the customer with developing data transmission and exchange controls to meet requirements. All data exchanges between systems or to third parties must be approved by the customer.	
56	**§164.312(c)(2)**	**Addressable Implementation Specification: Mechanism to Authenticate EPHI** Company has implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.	Cloud Vendor: 0% Lumen21: 75% Customer: 25%	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.	Lumen21 performs continuous monitoring of the customer's cloud environment, including configuration changes and perimeter monitoring to quickly identify potential changes in security operations. Any security, contractual, and regulatory requirements for data exchange are defined and documented as part of the onboarding process and included in the implementation plans. Lumen21 will assist the customer with developing data transmission and exchange controls to meet requirements. All data exchanges between systems or to third parties must be approved by the customer.	The Lumen21 Compliant Cloud Computing environment provides infrastructure services. Application-specific security controls are the responsibility of the customer and the application developer. The customer is responsible for informing Lumen21 of any application-specific logs that should be monitored.
57	**§164.312(d)**	**Required Standard: Person or Entity Authenticatio**	Cloud Vendor: 30% Lumen21: 60% Customer: 10%	Third party audit documents should provide evidence that the Cloud Vendor uses secure two-factor authentication for remote	Multi-Factor Authentication is provided for all remote access as a standard for	The customer is responsible for person or entity authentication for the customer

		n Company has implemented procedures to verify that a person or entity seeking access to EPHI is the one claimed.		access, and uses sufficiently complex controls for on-site access to properly authenticate users.	Lumen21 Compliant Cloud Computing Environment. All administrative access will require two-factor authentication.	business functions that require access to, creation or modification of, or transmission and storage of PHI, and any technical or physical environments containing PHI that are not managed by Lumen21.
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% Lumen21: 90% Customer: 10%	Customers are usually responsible for implementing encryption in transit using additional cryptographic services.	All incoming and outgoing network communications in the Lumen21 Compliant Cloud Computing environment is encrypted at all times.	The customer is responsible for transmission security for any technical or physical environments containing PHI that are not managed by Lumen21.
59	**§164.312(e)(2)(i)**	**Addressable Implementation Specification: Integrity Controls** Company has implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.	Cloud Vendor: 0% Lumen21: 90% Customer: 10%	Customers are usually responsible for implementing encryption in transit using additional cryptographic services.	All incoming and outgoing network communications in the Lumen21 Compliant Cloud Computing environment is encrypted at all times.	The customer is responsible for transmission security for any technical or physical environments containing PHI that are not managed by Lumen21.

#	Regulation Section	Standard/Implementation Specification	Cloud Computing HIPAA Compliance Responsibility	Cloud Vendor Security Controls	Lumen21 Security Controls	Customer Security Controls
ADMINISTRATIVE SAFEGUARDS						
60	**§164.312(e)(2)(ii)**	**Addressable Implementation Specification: Encryption** Company has implemented a mechanism to encrypt EPHI whenever deemed appropriate.	Cloud Vendor: 0% Lumen21: 90% Customer: 10%	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.	All Storage will be Encrypted and the keys will be stored in Authentication Systems or Third Party Key Management Software. All encryption keys will be owned by the data owner, and key management responsibilities will be identified during implementation. All incoming and outgoing network communications in the Lumen21 Compliant Cloud Computing environment is encrypted at all times.	The customer is responsible for appropriate encryption for any technical or physical environments containing PHI that are not managed by Lumen21.

HIPAA Compliance is a Shared Responsibility



The Lumen21-enabled cloud computing solution provides businesses with the opportunity to meet their security and regulatory needs. Learn more about the award-winning Lumen21 and its industry-recognized compatible solutions by visiting www.Lumen21.com or contacting us a sales@Lumen21.com