HIPAA SERVICES SCHEDULE

This HIPAA Services Schedule (or "**Product Terms**") to the GSA provides additional terms and conditions under which Customer has elected to purchase certain Rackspace Compliance Package – HIPAA Edition Services ("**HIPAA Security Package**") from Rackspace as more particularly described herein. Unless otherwise defined herein, capitalized terms shall have the meanings ascribed to them in the GSA and in the HIPAA Business Associate Agreement attached as Exhibit B ("**BAA**"), as the case may be. The scope of this schedule shall only apply to system components on Rackspace premises, managed by Rackspace and expressly agreed by the parties.

DEFINITIONS:
For the purposes of this HIPAA Services Schedule:

(i) any reference to the "GSA" shall mean the relevant agreement or any online terms and conditions in place between Rackspace and Customer;
(ii) any reference to "Rackspace" shall mean Rackspace US, Inc. or any Rackspace affiliate, subsidiary, assign or company;
(iii) any reference to "Customer" shall mean any customer (or "Customer", as may be defined in the GSA) or entity that contracted with Rackspace under the GSA or any online terms and conditions.

ADDITIONAL GENERAL TERMS AND CONDITIONS: The following provisions shall be in addition to or supplement the corresponding provisions in the GSA, as the case may be:

1. HIPAA COMPLIANCE SECURITY SERVICES.
The HIPAA Security Package can aid Customer in the protection of electronic protected healthcare information ("**PHI**") data and reduce overall system risk. The HIPAA Security Package encompasses certain technical safeguards together with associated policies and procedures to ensure controls are implemented and maintained. Rackspace designed the HIPAA Security Package based on industry standard best practices (e.g. HIPAA DSS), Rackspace's risk analysis results and the defense in depth approach. Rackspace's risk assessment was scoped to various segments of its network, including but not limited to its global management infrastructure. Additionally, Rackspace has assessed the theoretical risk of existing and future HIPAA Customers by utilizing a "typical" HIPAA-hosted architecture as a baseline. The HIPAA Security Package has been assembled to address these associated risks and reduce them to an acceptable level. Customer must perform an independent risk assessment to take into account issues, including, but not limited to those related to its applications, quantity and type of data, and deviations from a standard 3-tier public facing web application. If the elected Rackspace managed security controls encompassing the HIPAA Security Package are found to be insufficient in accordance with the Customer risk assessment or Customer-defined data classification protection levels, Customer must augment solution security with additional Customer-managed security controls as may be appropriate for Covered Entities or Business Associates.

While Rackspace treats all Customer data as confidential, it does not classify Customer data. The sensitivity levels of data must be defined and classified by Customer. Rackspace makes certain optional technical safeguards available to Customer, as detailed in the "Managed Security Service" column of Exhibit A, and which can be elected to address those HIPAA requirements ("**Requirements**") more specifically detailed in the responsibilities matrix set forth in Exhibit A. Rackspace only assumes responsibility for those security controls specifically identified in a Service Order (which may also be referred to as an Order Form). Customer will be solely responsible for addressing any Requirements that require utilization of a Rackspace Managed Security Service where Customer has elected not to purchase such service from Rackspace. Customer acknowledges Rackspace is providing only certain documented administrative and technical controls, which controls may not necessarily address all sub-requirements mandated by HIPAA. Accordingly, Customer assumes full responsibility for any gaps

©2018 Rackspace, US Inc. — Global Terms - March 2018 Revision OT#49979

between Rackspace's offering and the Security Standards, as identified in Customer's risk assessment, taking into account Rackspace's security policies.

Customer acknowledges Rackspace is not a "key custodian" as that term is utilized in the HIPAA DSS unless Customer utilizes a Rackspace managed service to encrypt data stored in a file and/or database (with such file, databases, tables, and columns requiring encryption identified by Customer in writing) by leveraging either Oracle Enterprise with Advanced Security Licensing or Microsoft SQL Enterprise ("**TDE**"), or Rackspace's File Encryption service. Customer shall not at any time share unencrypted Customer PHI data with Rackspace. If Customer does not utilize TDE or Rackspace's File Encryption service, Customer agrees it shall not share any encryption keys with Rackspace. Customer understands that as a Covered Entity or Business Associate (as the case may be), it has certain responsibilities under the law and has accordingly implemented internal administrative and technical safeguards to govern and protect PHI in order to comply with the Joint and Customer responsibilities set forth on Exhibit A. Customer agrees that if it declines to elect a particular optional service, then Customer shall have full responsibility for implementing that service. In the event Customer declines to elect any controls comprising the HIPAA Security Package, Customer acknowledges that Rackspace's ability to detect and respond to a security breach is diminished due to the absence of such controls. Furthermore, Customer understands and agrees that for those Requirements associated with declined security services that Rackspace shall not provide such technical controls and Customer is fulfilling its legal obligations under HIPAA by implementing and managing those technical controls itself.

The HIPAA Security Package does not include any network, storage, backup, or any other non-security hardware or software components. Accordingly, to satisfy any applicable local and offsite data backup HIPAA requirements, Customer must elect such services separately based on its specific data retention and business continuity requirements.

As a Business Associate providing managed services, Rackspace may have access to Customer data, including PHI. Rackspace does not however use or disclose Customer data, including PHI, as a part of any business practice. Rackspace shall only disclose PHI to Customer or in response to a lawful request for such disclosure, and in such instance only upon prior notice to Customer to the extent same is legally permissible.

The Parties have agreed to enter into a BAA in the form attached as Exhibit B.

2. TERM AND PAYMENT

Upon the expiration of each initial term of the HIPPA Security Package Services as set out in the Service Order, the HIPPA Security Package Services under this HIPPA Services Schedule shall be subject to automatic renewal for the same period as the initial term (or any agreed upon renewal term) unless: (i) Customer notifies Rackspace in writing of its intent to terminate the HIPPA Security Package Services no less than 30 days prior to the end of the then current term, or (ii) Rackspace notifies Customer in writing of its intent to terminate the HIPPA Security Package Services no less than 30 days prior to the end of the then current term. Customer shall pay Rackspace for all HIPPA Security Package Services through and including the date of termination. In the event Customer's customer or end-user is the United States Federal Government, the renewal term may be subject to the period of performance (base period and any exercised option periods) set by the Customer's Federal Government customer or end-user.

The monthly recurring fee together with any fees specified on the Service Order shall be billed to Customer via invoice in advance for HIPPA Security Package Services under this HIPPA Service Schedule to be provided for the following calendar month, unless otherwise specified in the Service Order. Nonrecurring fees including set-up fees shall be billed as incurred in any given month and fees for consumption-based HIPPA Security Package Services, if any, under this HIPPA Services Schedule such as conditioned power use overages or bandwidth use overages shall be invoiced in arrears ("Additional Fees").

Rackspace shall not raise the monthly recurring fee or minimum monthly recurring fee for HIPPA Security Package Services provided under this HIPPA Services Schedule before the expiration of the initial term of these HIPPA Security Package Services, except in the case of a material change in the HIPPA Security Package Services agreed to in writing by both Parties or a change in pricing due to a Third Party Fee Increase incurred by Rackspace in connection with the provision of the HIPPA Security Package Services. At least sixty (60) days prior to the conclusion of the then current term of the HIPPA Security Package Services, Rackspace shall inform Customer of any proposed increase in fees for HIPPA Security Package Services to go into effect as of the renewal date ("Increase Notice"). Notwithstanding the foregoing, Customer shall have 60 days' after receipt of the Increase Notice in which to terminate the HIPPA Security Package Services by providing Rackspace with written notice of termination ("Increase Termination Notice"). Should Customer fail to provide the Increase Termination Notice within this 60-day period, Customer shall have waived its right to terminate and the monthly recurring fee increase shall be in effect for the remainder of the renewal term. Any such increases accepted by Customer shall be effective as of the next monthly remittance date after the expiration of the 60-day notice period. In the case of a material change in the HIPPA Security Package Services, the Parties will execute a Service Order or other form of written amendment.

3. REVISION HISTORY

Revision Level	History	Revision Date
1	Initial Release	09-15-2014
2	Incorporated PCI DSS v3.1 as the HIPAA risk management framework	10-11-2016
3	Definitions section added, minor changes to Responsibility Breakdown	03-30-2017
4	Updated to reflect corporate structure	03-14-2018

[THE BALANCE OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

GENERAL REQUIREMENT RESPONSIBILITIES

*This Exhibit specifies the HIPAA Requirements for the HIPAA Security Package Services and delineates, in the Requirement Responsibility column for each Requirement, which Party is responsible for each of the Requirements. In some instances, a Requirement is listed as solely the responsibility of Rackspace or Customer, and in other instances it is the responsibility of both Parties, in which case the Requirement is listed herein as "Joint". The listing in the Requirement Responsibility column, and the associated responsibility for each Requirement, is referred to as a Party's "**Responsibility**".*

In Customer elects not to purchase for its HIPAA Services, or subsequently removes from its HIPAA Services any of the services listed for each of the Requirements under the Managed Security Service column, the Responsibility for each Requirement associated with each such Managed Security Service shall immediately become the Responsibility of Customer regardless of whether the Responsibility is listed as "Rackspace" or "Joint".

BUILD AND MAINTAIN A SECURE NETWORK

Requirement 1: Install and maintain a firewall configuration to protect PHI data.

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The PHI data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the PHI data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

Requirement Number ("Requirement")	Requirement Description	Requirement Responsibility	Managed Security Service
1.1	Establish and implement firewall and router configuration standards that include the following:	Section Header	
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	Joint	Dependent on Managed Firewall
1.1.2	Current network diagram that identifies all connections between the PHI data environment and other networks, including any wireless networks	Joint	
1.1.3	Current diagram that shows all PHI data flows across systems and networks	Customer	
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Rackspace	Managed Firewall
1.1.5	Description of groups, roles, and responsibilities for management of network components	Rackspace	Dependent on Managed Firewall
1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.	Joint	Dependent on Managed Firewall

1.1.7	Requirement to review firewall and router rule sets at least every six months	Joint	Firewall Review
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the PHI data environment. ***Note**: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	Section Header	
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the PHI data environment, and specifically deny all other traffic.	Joint	Managed Firewall
1.2.2	Secure and synchronize router configuration files.	Rackspace	
1.2.3	Install perimeter firewalls between all wireless networks and the PHI data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the PHI data environment	Not Applicable	
1.3	Prohibit direct public access between the Internet and any system component in the PHI data environment	Section Header	
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Rackspace	Managed Firewall
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	Joint	Managed Firewall
1.3.3	Do not allow any direct connections inbound or outbound for traffic between the Internet and the PHI data environment.	Joint	Managed Firewall
1.3.4	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	Rackspace	Managed Firewall
1.3.5	Do not allow unauthorized outbound traffic from the PHI data environment to the Internet.	Rackspace	Managed Firewall
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	Rackspace	Managed Firewall
1.3.7	Place system components that store PHI data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Joint	Managed Firewall

1.3.8	Do not disclose private IP addresses and routing information to unauthorized parties. ***Note**: Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT)* • *Placing servers containing PHI data behind proxy servers/firewalls.* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	Rackspace	Managed Firewall
1.4	Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: • Specific configuration settings are defined for personal firewall software. • Personal firewall software is actively running. • Personal firewall software is not alterable by users of mobile and/or employee-owned devices	Not Applicable or Customer	
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Joint	Managed Firewall

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.			
Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.			
Requirement Number ("Requirement")	**Requirement Description**	**Requirement Responsibility**	**Managed Security Service**
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.)	Joint	
2.1.1	For wireless environments connected to the PHI data environment or transmitting PHI data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Not Applicable or Customer	
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	Rackspace	Continuous Audit
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) *Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.*	Joint	
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Joint	Continuous Audit

2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc. Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.	Joint	
2.2.4	Configure system security parameters to prevent misuse.	Rackspace	Continuous Audit
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Rackspace	Continuous Audit
2.3	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access. Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.	Joint	
2.4	Maintain an inventory of system components that are in scope for HIPAA	Customer	
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Joint	
2.6	Shared hosting providers must protect each entity's hosted environment and PHI data. These providers must meet specific requirements as detailed in Appendix A: Additional HIPAA Requirements for Shared Hosting Providers.	Not Applicable or Customer	

PROTECT PHI DATA

Requirement 3: Protect stored PHI data.

Protection methods such as encryption, truncation, masking, and hashing are critical components of PHI data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing PHI data unless absolutely necessary, truncating PHI data if full PHI is not needed, and not sending unprotected PHI using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for definitions of "strong cryptography" and other PCI DSS terms.

Requirement Number ("Requirement")	Requirement Description	Requirement Responsibility	Managed Security Service
3.1	Keep PHI data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all PHI data (PHI) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for PHI data • A quarterly process for identifying and securely deleting stored PHI data	Customer	
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • *There is a business justification and* • *The data is stored securely.* Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	Not Applicable	

3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note**: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*	Not Applicable	
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	Not Applicable	
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	Not Applicable	
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN. ***Note:** This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	Not Applicable	
3.4	Render PHI unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	Rackspace[i,ii]	TDE and/or Rackspace's File Encryption Service

3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	Not Applicable or Customer	
3.5	Document and implement procedures to protect keys used to secure stored PHI data against disclosure and misuse: ***Note**: This requirement applies to keys used to encrypt stored PHI data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*	Joint[iii,iv]	TDE and/or Rackspace's File Encryption Service
3.5.1	Restrict access to cryptographic keys to the fewest number of custodians necessary.	Joint[iii,iv]	TDE and/or Rackspace's File Encryption Service
3.5.2	Store secret and private keys used to encrypt/decrypt PHI data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares. In accordance with an industry-accepted method ***Note**: It is not required that public keys be stored in one of these forms.*	Joint[iii]	TDE and/or Rackspace's File Encryption Service
3.5.3	Store cryptographic keys in the fewest possible locations.	Joint[iii,iv]	TDE and/or Rackspace's File Encryption Service
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of PHI data, including the following: ***Note**: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	Section Header	
3.6.1	Generation of strong cryptographic keys	Rackspace[iii]	TDE and/or Rackspace's File Encryption Service
3.6.2	Secure cryptographic key distribution	Joint[iii,iv]	TDE and/or Rackspace's File Encryption Service
3.6.3	Secure cryptographic key storage	Joint[iii,iv]	TDE and/or Rackspace's File Encryption Service

3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	Joint[iii]	TDE and/or Rackspace's File Encryption Service
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. ***Note**: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	Joint[iii,iv]	TDE and/or Rackspace's File Encryption Service
3.6.6	If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control. ***Note**: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	Not Applicable or Customer	
3.6.7	Prevention of unauthorized substitution of cryptographic keys.	Rackspace[iii]	TDE and/or Rackspace's File Encryption Service
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	Joint[iii,iv]	TDE and/or Rackspace's File Encryption Service
3.7	Ensure that security policies and operational procedures for protecting stored PHI data are documented, in use, and known to all affected parties.	Joint	

Requirement 4: Encrypt transmission of PHI data across open, public networks.			
Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to PHI data environments.			
Requirement Number ("Requirement")	**Requirement Description**	**Requirement Responsibility**	**Managed Security Service**
4.1	Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive PHI data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016. Examples of open, public networks include but are not limited to: • The Internet • Wireless technologies, including 802.11 and Bluetooth • Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA) General Packet Radio Service (GPRS) Satellite communications	Joint	
4.1.1	Ensure wireless networks transmitting PHI data or connected to the PHI data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. ***Note**: The use of WEP as a security control was prohibited as of 30 June 2010.*	Not Applicable or Customer	
4.2	Never send unprotected PHI by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	Joint	
4.3	Ensure that security policies and operational procedures for encrypting transmissions of PHI data are documented, in use, and known to all affected parties.	Customer	

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

Requirement Number ("Requirement")	Requirement Description	Requirement Responsibility	Managed Security Service
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Rackspace[v]	Anti-Virus/Anti-Malware
5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Rackspace[v]	Anti-Virus/Anti-Malware
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Joint	
5.2	Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per HIPAA Requirement 10.7.	Rackspace[v]	Anti-Virus/Anti-Malware
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. ***Note**: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active*	Rackspace[v]	Anti-Virus/Anti-Malware
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties	Joint	

Requirement 6: Develop and maintain secure systems and applications.

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of PHI data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

Requirement Number ("Requirement")	Requirement Description	Requirement Responsibility	Managed Security Service
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note**: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit PHI data.*	Joint	Patch Management
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Note:** Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	Joint	Patch Management
6.3	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with HIPAA (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle ***Note:** this applies to all software developed internally as well as bespoke or custom software developed by a third party.*	Customer	

6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Customer	
6.3.2	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. ***Note**: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle.* *Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at HIPAA Requirement 6.6.*	Customer	
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:	Section Header	
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	Joint	
6.4.2	Separation of duties between development/test and production environments	Customer	
6.4.3	Production data (live PHI) are not used for testing or development	Customer	
6.4.4	Removal of test data and accounts before production systems become active	Customer	
6.4.5	Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	Section Header	
6.4.5.1	Documentation of impact.	Joint	Advanced Change Control
6.4.5.2	Documented change approval by authorized parties.	Joint	Advanced Change Control
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.	Joint	Advanced Change Control
6.4.5.4	Back-out procedures.	Joint	Advanced Change Control

6.5	Address common coding vulnerabilities in software-development processes as follows: • Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. • Develop applications based on secure coding guidelines. ***Note**: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of HIPAA was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*	Customer	
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Customer	
6.5.2	Buffer overflows	Customer	
6.5.3	Insecure cryptographic storage	Customer	
6.5.4	Insecure communications	Customer	
6.5.5	Improper error handling	Customer	
6.5.6	All "High" vulnerabilities identified in the vulnerability identification process (as defined in HIPAA Requirement 6.1).	Customer	
***Note**: Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):*			
6.5.7	Cross-site scripting (XSS)	Customer	
6.5.8	Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal, and failure to restrict user access to functions)	Customer	
6.5.9	Cross-site request forgery (CSRF)	Customer	
6.5.10	Broken authentication and session management ***Note**: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*	Customer	

6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ***Note**: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic	Rackspace	Web Application Firewall (WAF)
6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	Joint	

IMPLEMENT STRONG ACCESS CONTROL MEASURES			
Requirement 7: Restrict access to PHI data by business need to know.			
To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. *"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.*			
Requirement Number ("Requirement")	**Requirement Description**	**Requirement Responsibility**	**Managed Security Service**
7.1	Limit access to system components and PHI data to only those individuals whose job requires such access.	Joint	
7.1.1	Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.	Joint	
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Joint	
7.1.3	Assign access based on individual personnel's job classification and function.	Joint	
7.1.4	Require documented approval by authorized parties specifying required privileges.	Joint	
7.2	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	Section Header	
7.2.1	Coverage of all system components	Joint	
7.2.2	Assignment of privileges to individuals based on job classification and function	Joint	
7.2.3	Default "deny-all" setting ***Note**: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*	Joint	
7.3	Ensure that security policies and operational procedures for restricting access to PHI data are documented, in use, and known to all affected parties.	Joint	

Requirement 8: Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

***Note:** These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access PHI data or to access systems with PHI data. This includes accounts used by vendors and other third parties (for example, for support or maintenance).*

However, Requirements 8.1.1, 8.2, 8.5, 8.2.3 through 8.2.5, and 8.1.6 through 8.1.8 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

Requirement Number ("Requirement")	Requirement Description	Requirement Responsibility	Managed Security Service
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	Section Header	
8.1.1	Assign all users a unique ID before allowing them to access system components or PHI data.	Joint	
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Joint	
8.1.3	Immediately revoke access for any terminated users.	Joint	
8.1.4	Remove/disable inactive user accounts within 90 days.	Joint[vi]	Dependent on 2-Factor Authentication
8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	Joint	
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Rackspace	Dependent on Continuous Audit
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Rackspace	Dependent on Continuous Audit
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Rackspace	Dependent on Continuous Audit

8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	Joint	
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Joint	
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	Joint	
8.2.3	Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	Rackspace	Dependent on Continuous Audit
8.2.4	Change user passwords/passphrases at least every 90 days.	Joint	Dependent on Continuous Audit
8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	Rackspace	Dependent on Continuous Audit
8.2.6	Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	Joint	
8.3	Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance). ***Note**: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.* *Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.*	Rackspace	2-factor Authentication

8.4	Document and communicate authentication procedures and policies to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	Joint	
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	Joint	
8.5.1	***Additional requirement for service providers:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. ***Note:*** *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.* ***Note****: Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement.*	Rackspace	
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Rackspace	Dependent on 2-Factor Authentication
8.7	All access to any database containing PHI data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	Joint	

8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	Joint	

Requirement 9: Restrict physical access to PHI data.			
Any physical access to data or systems that house PHI data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing PHI data.			
Requirement Number ("Requirement")	**Requirement Description**	**Requirement Responsibility**	**Managed Security Service**
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the PHI data environment.	Rackspace	
9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note**: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit PHI data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	Rackspace	
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	Rackspace	
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	Rackspace	
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	Rackspace	
9.3	Control physical access for onsite personnel to the sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	Rackspace	
9.4	Implement procedures to identify and authorize visitors. Procedures should include the following:	Section Header	

9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where PHI data is processed or maintained.	Rackspace	
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	Rackspace	
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	Rackspace	
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where PHI data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	Rackspace	
9.5	Physically secure all media.	Joint	
9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Joint	
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:	Section Header	
9.6.1	Classify media so the sensitivity of the data can be determined.	Joint	
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	Joint	
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	Joint	
9.7	Maintain strict control over the internal or external distribution of any kind of media, including the following:	Section Header	
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	Joint	
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:	Section Header	
9.8.1	Shred, incinerate, or pulp hard-copy materials so that PHI data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	Customer	
9.8.2	Render PHI data on electronic media unrecoverable so that PHI data cannot be reconstructed.	Joint	

9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note**: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.* ***Note**: Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.*	Not Applicable	
9.9.1	Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.	Not Applicable	
9.9.2	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). ***Note**: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.*	Not Applicable	
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Not Applicable	
9.10	Ensure that security policies and operational procedures for restricting physical access to PHI data are documented, in use, and known to all affected parties.	Joint	

REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and PHI data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

Requirement Number ("Requirement")	Requirement Description	Requirement Responsibility	Managed Security Service
10.1	Implement audit trails to link all access to system components to each individual user.	Joint	
10.2	Implement automated audit trails for all system components to reconstruct the following events:	Section Header	
10.2.1	All individual user accesses to PHI data	Joint[i]	TDE and/or Rackspace's File Encryption Service
10.2.2	All actions taken by any individual with root or administrative privileges	Joint[vii]	Dependent on Event Management
10.2.3	Access to all audit trails	Rackspace[vii]	Event Management
10.2.4	Invalid logical access attempts	Rackspace	Continuous Audit
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	Rackspace	Continuous Audit
10.2.6	Initialization, stopping, or pausing of the audit logs	Rackspace	Continuous Audit
10.2.7	Creation and deletion of system-level objects	Rackspace	Continuous Audit
10.3	Record at least the following audit trail entries for all system components for each event:	Section Header	
10.3.1	User identification	Rackspace[vii]	Dependent on Continuous Audit
10.3.2	Type of event	Rackspace[vii]	Dependent on Continuous Audit
10.3.3	Date and time	Rackspace[vii]	Dependent on Continuous Audit
10.3.4	Success or failure indication	Rackspace[vii]	Dependent on Continuous Audit
10.3.5	Origination of event	Rackspace[vii]	Dependent on Continuous Audit
10.3.6	Identity or name of affected data, system component, or resource.	Rackspace[vii]	Dependent on Continuous Audit

10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note**: One example of time synchronization technology is Network Time Protocol (NTP).*	Rackspace	
10.4.1	Critical systems have the correct and consistent time.	Rackspace	
10.4.2	Time data is protected.	Rackspace	Dependent on Continuous Audit
10.4.3	Time settings are received from industry-accepted time sources.	Rackspace	
10.5	Secure audit trails so they cannot be altered.	Section Header	
10.5.1	Limit viewing of audit trails to those with a job-related need.	Joint[vii]	Dependent on Event Management
10.5.2	Protect audit trail files from unauthorized modifications.	Rackspace[vii]	Dependent on Event Management
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter	Rackspace[vii]	Dependent on Event Management
10.5.4	Write logs for external-facing technologies onto a log server on the internal LAN.	Rackspace[vii]	Dependent on Event Management
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Rackspace[vii]	Dependent on Event Management
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note**: Log harvesting, parsing, and alerting tools may be used to meet this Requirement*.	Section Header	
10.6.1	Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit PHI and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Joint[vii,viii]	Event Management
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	Joint[vii,viii]	Event Management

10.6.3	Follow up exceptions and anomalies identified during the review process.	Joint	Event Management
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	Rackspace[vii]	Event Management
10.8	Ensure that security policies and operational procedures for monitoring all access to network resources and PHI data are documented, in use, and known to all affected parties.	Joint	

Requirement 11: Regularly test security systems and processes.			
Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.			
Requirement Number ("Requirement")	**Requirement Description**	**Requirement Responsibility**	**Managed Security Service**
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note**: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*	Rackspace	
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.	Rackspace	
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.	Rackspace	
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note**: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial HIPAA compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial HIPAA review, four quarters of passing scans must have occurred.*	Section Header	
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	Joint	Vulnerability Assessment
11.2.2	Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note**: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	Joint	Intrusion Detection Service

11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	Joint	Dependent on Vulnerability Assessment and Intrusion Detection Service
11.3	Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results. ***Note**: This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. HIPAA v2.0 requirements for penetration testing must be followed until v3.0 is in place.*	Customer	
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Customer	
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment)	Customer	
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	Customer	
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Customer	

11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the PHI data environment as well as at critical points in the PHI data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Rackspace	Intrusion Detection Services
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note**: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*	Rackspace	Continuous Audit
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.	Joint	Continuous Audit
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Joint	

MAINTAIN AN INFORMATION SECURITY POLICY			
Requirement 12: Maintain a policy that addresses information security for all personnel.			
A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the PHI data environment.			
Requirement Number ("Requirement")	**Requirement Description**	**Requirement Responsibility**	**Managed Security Service**
12.1	Establish, publish, maintain, and disseminate a security policy.	Joint	
12.1.1	Review the security policy at least annually and update the policy when the environment changes.	Joint	
12.2	Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800 30.	Joint	
12.3	Develop usage policies for critical technologies and define proper use of these technologies. ***Note**: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* Ensure these usage policies require the following:	Section Header	
12.3.1	Explicit approval by authorized parties	Joint	
12.3.2	Authentication for use of the technology	Joint	
12.3.3	A list of all such devices and personnel with access	Joint	
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	Joint	
12.3.5	Acceptable uses of the technology	Joint	
12.3.6	Acceptable network locations for the technologies	Joint	
12.3.7	List of company-approved products	Joint	
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Joint	Continuous Audit
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	Joint	

12.3.10	For personnel accessing PHI data via remote-access technologies, prohibit the copying, moving, and storage of PHI data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable HIPAA Requirements.	Joint	
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Joint	
12.5	Assign to an individual or team the following information security management responsibilities:	Section Header	
12.5.1	Establish, document, and distribute security policies and procedures.	Joint	
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Joint	
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	Joint	
12.5.4	Administer user accounts, including additions, deletions, and modifications	Joint	
12.5.5	Monitor and control all access to data.	Joint	
12.6	Implement a formal security awareness program to make all personnel aware of the importance of PHI data security.	Joint	
12.6.1	Educate personnel upon hire and at least annually. ***Note**: Methods can vary depending on the role of the personnel and their level of access to the PHI data.*	Joint	
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Joint	
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) ***Note**: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	Joint	
12.8	Maintain and implement policies and procedures to manage service providers with whom PHI data is shared, or that could affect the security of PHI data, as follows:	Section Header	
12.8.1	Maintain a list of service providers.	Customer	

12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of PHI data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's PHI data environment. ***Note**: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	Joint	
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Customer	
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Not Applicable	
12.8.5	Maintain information about which HIPAA requirements are managed by each service provider, and which are managed by the entity.	Customer	
12.9	**Additional requirement for service providers only**: Service providers acknowledge in writing to customers that they are responsible for the security of PHI data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's PHI data environment. ***Note**: This requirement is a best practice until June 30, 2015, after which it becomes a requirement.* ***Note**: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	Rackspace	
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.	Section Header	

12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.	Joint	
12.10.2	Test the plan at least annually.	Joint	
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Joint	
12.10.4	Provide appropriate training to staff with security breach response responsibilities.	Joint	
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	Joint	
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Joint	

[i] *Rackspace's responsibility pertains only to PHI secured via TDE and/or Rackspace's File Encryption Service.*

[ii] *Rackspace's responsibility pertains only to those files, databases, tables and/or columns specified by Customer to Rackspace in writing as requiring such encryption.*

[iii] *Rackspace's responsibility pertains only to those encryption keys which are utilized by TDE and/or the wrapper keys utilized by Rackspace's File Encryption Service to protect the DSM configuration backup.*

[iv] *Rackspace may send encrypted TDE key backups and/or Rackspace's File Encryption wrapper keys and associated DSM backups to Customer for business continuity purposes. If Customer doesn't wish to accept receipt of aforementioned items, then responsibility shall be solely Rackspace's.*

[v] *Rackspace does not include Anti-Virus/Anti-Malware as a part of its PCI package for Unix/Linux based systems. Rackspace recommends Customer perform a risk assessment to determine risk and if such systems are commonly affected by malicious software. In the event Customer determines such systems are commonly affected, Customer must request Anti-Virus/Anti-Malware services be added to the affected systems.*

[vi] *Rackspace will not remove/disable inactive accounts on servers as this may have a negative impact on production systems and Customer is solely responsible for such activity. Rackspace's 2-Factor Authentication service can be configured such that inactive VPN accounts are disabled after a specified period of time.*

[vii] *Only pertains to audit trails written to Rackspace's Event Management service.*

[viii] *Only pertains to log types Supported by Alert Logic Log Review service.*

APPENDIX A: ADDITIONAL HIPAA REQUIREMENTS FOR SHARED HOSTING PROVIDERS			
Requirement A.1: Shared hosting providers must protect the PHI data environment			
As referenced in Requirement 12.8 and 12.9, all service providers with access to PHI data (including shared hosting providers) must adhere to HIPAA . In addition, Requirement 2.6 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.			
Requirement Number ("Requirement")	**Requirement Description**	**Requirement Responsibility**	**Managed Security Service**
A.1	Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of HIPAA. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with HIPAA and validate compliance as applicable.	Not Applicable or Customer	
A.1.1	Ensure that each entity only runs processes that have access to that entity's PHI data environment.	Not Applicable or Customer	
A.1.2	Restrict each entity's access and privileges to its own PHI data environment only.	Not Applicable or Customer	
A.1.3	Ensure logging and audit trails are enabled and unique to each entity's PHI data environment and consistent with HIPAA Requirement 10.	Not Applicable or Customer	
A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	Not Applicable or Customer	

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
1.1	Section Header
1.1.1	Rackspace is responsible for following a process of seeking approval before implementing any firewall or router configuration changes. Customer is responsible for approving all changes requested by Customer and implemented by Rackspace.
1.1.2	Rackspace is responsible for creating and delivering an initial network diagram for any new HIPAA solution architected by Rackspace. For any existing managed solution, Rackspace will create or update a network diagram upon request, provided Customer supplies all relevant information for the diagram
1.1.3	It is the responsibility of the Customer to create a data flow diagram to demonstrate PHI data flows and disseminate to Rackspace for future topology related updates.
1.1.4	When Rackspace implements a Customer PHI data environment on its premises, if applicable the network design will leverage a DMZ/internal network architecture.
1.1.5	Rackspace is responsible for maintaining appropriate documentation to support this control describing the management responsibilities of network components under Rackspace's management.
1.1.6	Rackspace is responsible for the documentation and business justification for services, protocols, and ports required by Rackspace to implement its services which include optional security services, remote management, and monitoring of the Customer infrastructure. Customer is responsible for documentation of the same, for all other cases.
1.1.7	Rackspace shall review is documented business justified firewall rules pertaining to its security services, remote management, and monitoring for accuracy and necessity at least every six months, and provide notification to Customer in the event modifications are required. Customer shall do the same on any firewall rules implemented by Rackspace upon Customer request and approval. If Firewall review service is elected, detailed bi-annual reports will be delivered to the Customer to aid in this process.
1.2	Section Header
1.2.1	Rackspace is responsible for ensuring its business justified firewall rules are a necessity. Customer must do the same on the firewall rules requested by the Customer and implemented by Rackspace.
1.2.2	This is the responsibility of Rackspace.
1.2.3	Not Applicable to HIPAA
1.3	Section Header
1.3.1	Rackspace is responsible for implementing a DMZ based on written request and approval by Customer.
1.3.2	Rackspace is responsible for implementing specific firewall configurations to control traffic based on written request and approval by Customer.
1.3.3	Rackspace is responsible for implementing specific firewall configurations to control traffic based on written request and approval by Customer.
1.3.4	Responsibility of Rackspace by leveraging firewall configuration best practices.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
1.3.5	Rackspace is responsible for implementing specific firewall configurations to control traffic based on written request and approval by Customer.
1.3.6	Rackspace managed firewalls will leverage stateful inspection.
1.3.7	Rackspace is responsible for implementing an internal network zone based on written request and approval by Customer. Customer is responsible for ensuring only system components in this zone touch PHI.
1.3.8	This is the responsibility of Rackspace.
1.4	Rackspace does not allow mobile and/or employee-owned devices to connect directly to any Customers' solutions. Customer is responsible for this requirement to the extent it is applicable.
1.5	Both Rackspace and Customer are responsible for ensuring security policies and procedures based on applicable requirement 1 responsibilities.
2.1.	Rackspace is responsible for changing vendor-supplied defaults for Rackspace provided and managed security software, as well as system accounts leveraged by Rackspace for monitoring and management. Changing/disabling all other system defaults and unnecessary accounts is the responsibility of the Customer.
2.1.1	Rackspace wireless networks are not connected to Customer PHI environment or transmit PHI data. Customer is responsible for this requirement to the extent it is applicable.
2.2	Rackspace is responsible for developing industry accepted system hardening standards. Only those supported system components with Rackspace's optional Continuous Audit service shall have the standard implemented. Customer is responsible for all other unsupported system components, or system components without the Continuous Audit service.
2.2.1.	Each party shall not implement more than one primary function per server.
2.2.2	Rackspace is responsible for implementing its industry accepted hardening standard on those system components with Rackspace's optional Continuous Audit service. Customer is responsible for all other unsupported system components, or system components without the Continuous Audit service.
2.2.3.	Rackspace is responsible for not utilizing insecure services, protocols, or daemons in delivery of its services (monitoring, remote management, security services, etc.…). Rackspace to implement additional security features for any Customer required insecure services, protocols, or daemons upon request if feasible. Customer is responsible for this requirement for any Customer implemented insecure services, protocols, or daemons.
2.2.4.	Rackspace is responsible for implementing its industry accepted hardening standard on those system components with Rackspace's optional Continuous Audit service. Customer is responsible for all other unsupported system components, or system components without the Continuous Audit service
2.2.5.	Rackspace is responsible for implementing its industry accepted hardening standard on those system components with Rackspace's optional Continuous Audit service. Customer is responsible for all other unsupported system components, or system components without the Continuous Audit service

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
2.3.	Rackspace is responsible for ensuring all non-console administrative access is encrypted with strong cryptography for management interfaces required by Rackspace and additional interfaces agreed to by parties in writing. Customer is responsible for all other such management interfaces.
2.4.	The Customer is responsible for maintaining an inventory of its system components that are in scope for PCI DSS and for maintaining the scope and communicating that scope to Rackspace.
2.5.	Rackspace is responsible for documenting security policies and operational procedures in connection with its hardening standards as applicable to supported system components. Customer is responsible for requesting and approving deployment of such standards, as well as documentation and deployment for unsupported system components.
2.6.	Rackspace does not provide shared hosting to its Customers. Customer is responsible for this requirement to the extent it is applicable.
3.1.	Not Applicable to HIPAA environments.
3.2.	Not Applicable to HIPAA environments.
3.2.1.	Not Applicable to HIPAA environments.
3.2.2.	Not Applicable to HIPAA environments.
3.2.3.	Not Applicable to HIPAA environments.
3.3.	Not Applicable to HIPAA environments.
3.4.	Rackspace is responsible for encrypting PHI only if secured via its Transparent Data Encryption (TDE) and/or Rackspace's File Encryption Services. Customer is responsible for indicating to Rackspace in writing those file, databases, tables and/or columns requiring such encryption. Customer is responsible for securing PHI in all other stored locations.
3.4.1.	Rackspace does not currently support disk based encryption for HIPAA solutions on its premises. Customer is responsible for meeting this control should they choose to implement disk based encryption to secure PHI.
3.5.	Rackspace is responsible for documenting and implementing procedures to protect keys in connection with its services. Customer is responsible for such procedures for protecting keys in all other cases.
3.5.1	Each party is responsible for this requirement for any keys which such party is a key custodian.
3.5.2	Rackspace is responsible for securely storing private keys in connection with its services to the extent it's applicable. Customer is responsible for securely storing private keys in all other cases.
3.5.3	Each party is responsible for this requirement for any keys which such party is a key custodian.
3.6	Section Header
3.6.1	Rackspace is responsible for the generation of strong cryptographic keys in connection with its services. Customer is responsible for this requirement in all other cases.
3.6.2	Rackspace is responsible for the secure distribution of keys provided to the Customer in connection with its services to the extent it is applicable. Customer is responsible for this requirement in all other cases.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
3.6.3	Rackspace is responsible for secure cryptographic key storage in connection with its services to the extent it is applicable. Customer is responsible for this requirement in all other cases.
3.6.4	Rackspace is responsible for cryptographic key changes in connection with its services to the extent it is applicable. Customer is responsible for this requirement in all other cases.
3.6.5	Rackspace is responsible for the retirement or replacement of keys in connection with its services to the extent it is applicable. Customer is responsible for notifying Rackspace of key replacement as deemed necessary by the Customer. In addition, Customer is responsible for this requirement in all other cases not in connection with Rackspace's TDE service.
3.6.6	Rackspace does not leverage manual clear-text cryptographic key management in connection with its services. Customer is responsible for this requirement in all other cases.
3.6.7	Rackspace is responsible the prevention of unauthorized substitution of cryptographic keys in connection with its service services. Customer is responsible for this requirement in all other cases.
3.6.8	Rackspace is responsible for formally acknowledging key custodians in connection with its services. Customer is responsible for this requirement for keys outside of Rackspace services or when in receipt of key backup applicable to Rackspace services.
3.7	Each party is responsible for this requirement for such protection mechanisms applicable to the party as detailed in this document.
4.1	Rackspace is responsible for the implementation of the Customer provided cryptographic keys and/or protocols upon request and approval from Customer. Customer is responsible for choosing to leverage strong cryptography and security protocols.
4.1.1	Rackspace wireless networks are not connected to Customer PHI environment nor do they transmit PHI data. Customer is responsible for this requirement to the extent it is applicable.
4.2	Rackspace is responsible for implementing administrative policies and security awareness training to prohibit the sending of unprotected PHI over end-user messaging technologies. The Customer is responsible for implementing its own set of organizational policies.
4.3	Rackspace does not transmit PHI data on behalf of the Customer. The Customer is responsible for this requirement to the extent that it is applicable.
5.1	Rackspace is responsible for deploying its Anti-Malware service to supported system components upon Customer request and approval. Alternatively, Customer may deploy or embed Rackspace anti-virus packages on supported system templates/images. Customer is responsible for anti-virus on all other system components and on all personal computers.
5.1.1	Rackspace performs periodic reviews of vendor documentation to ensure applicability of current and emerging threats, and updates its antivirus software accordingly. The Customer is responsible for its own vendor evaluation of anti-virus programs not provided by Rackspace.
5.1.2	Both Rackspace and Customer to perform periodic risk assessments to determine applicability and necessity of anti-virus on all systems components considered not commonly affected. For Rackspace managed Anti-Malware service deployment, it is Customer's responsibility to specifically request and approve anti-virus for non-Windows systems.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
5.2	Rackspace to ensure all system components with Rackspace's elected Anti-Malware service will continuously function in accordance with its associated policy. Customer is responsible for the same mechanisms on personal computers and system components not leveraging Rackspace's anti-malware service.
5.3	Rackspace is responsible for implementing its Anti-Virus/Anti-Malware configuration policy to ensure active protection and restricted access to administrative areas of the program. Customer is responsible for the same when not leveraging Rackspace's anti-virus on systems components and/or personal computers.
5.4	Rackspace is responsible for developing security policies and procedures and ensuring its use and dissemination to all personnel. Customer is responsible for implementing its own organizational security policies.
6.1.	Rackspace is responsible for following its risk ranking process to identify security vulnerabilities in connection with supported operating systems and applications. Customer is responsible for following its risk ranking process for any unsupported operating systems and applications provided by or managed by Customer.
6.2.	Rackspace is responsible for installing critical vendor-supplied security patches for all supported system components within one month of release upon approval from Customer. Customer is responsible for installing patches for all other cases.
6.3.	Rackspace does not develop internal or external software applications to be used in the Customer PHI environment. Customer is responsible for this requirement.
6.3.1.	Rackspace does not develop internal or external software applications to be used in the Customer PHI environment. Customer is responsible for this requirement.
6.3.2.	Rackspace does not develop internal or external software applications to be used in the Customer PHI environment. Customer is responsible for this requirement.
6.4.	Section Header
6.4.1.	Rackspace is responsible for implementing access control mechanisms to enforce separation of development/test and production environments based on Customer provided information, request, and approval. Customer is responsible for doing the same for all development/test environments not implemented by Rackspace.
6.4.2.	Customer is responsible for separation of duties between development/test and production environments. Rackspace does not perform duties in connection with development/test environments. Therefore, such separation is not applicable.
6.4.3.	Customer is responsible for not utilizing production data (live PHI) for testing or development.
6.4.4.	Rackspace does not develop internal or external software applications to be used in the Customer PHI environment. Customer is responsible for this requirement.
6.4.5.	Section Header

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
6.4.5.1.	Rackspace is responsible for enforcing change control procedures through its ticketing system, and training to support personnel. Each party to document the impact to the extent known. Customer is responsible for such documentation for all changes made directly by Customer.
6.4.5.2.	Rackspace is responsible for seeking approval for all changes raised within its change control process. Customer is responsible for timely approvals as appropriate.
6.4.5.3.	Each party to test functionality within its functional area of responsibility.
6.4.5.4.	Each party to document the back-out procedures as may be appropriate for that party, depending on the nature of the change. For example, if Customer raises a change control request with detailed procedures for making such change, Customer to also provide back-out procedures. If change procedures are covered under managed services, Rackspace to document such back-out procedures.
6.5.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.1.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.2.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.3.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.4.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.5.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.6.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.7.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.8.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.9.	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.5.10	Customer is responsible for addressing common coding vulnerabilities for all custom software
6.6	Rackspace is responsible for implementing a web application firewall (WAF) for all web sites subscribing to Rackspace's optional WAF service. Customer is responsible for implementing manual/automated code review or web application firewall for all other cases.
6.7	Rackspace is responsible for documenting security policies and operational procedures for maintaining secure systems for supported system components. Customer is responsible for security policies in connection with development as well as system maintenance for any system components maintained by Customer.
7.1	Rackspace is responsible for limiting employee access to resources based on his/her job responsibilities. Customer is responsible for ensuring its own employee access control policy.
7.1.1	Rackspace is responsible for defining all departmental roles within the organization and the level of access required to perform its job functions. Customer is responsible for defining all roles within its organization and subsequent access.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
7.1.2	Rackspace follows a least privilege security principle to ensure permissions to users are not granted beyond the scope of the necessary rights required to perform their job functions. Customer is responsible for implementing its own access control policy.
7.1.3	Rackspace assigns access to personnel by leveraging a role based access control authorization model. Customer is responsible for implementing its own access control model or policy.
7.1.4	Rackspace Human Resources is responsible for ensuring employee access requests are documented and validated against departmental roles. Customer is responsible for implementing its own organizational access control policy.
7.2	Section Header
7.2.1	Rackspace requires Customer environment to provide a functioning access control system (i.e. Active Directory, OpenLDAP, local OS accounts, etc.…). Rackspace is responsible implementing an access control system upon request as may be supported by the system components. Customer is responsible for ensuring all non-Rackspace managed system components, and all other system components not covered by Rackspace managed and Customer provided access control systems, meet this requirement.
7.2.2	Rackspace is responsible for assigning privileges to its employees based on their job responsibilities. Customer is responsible for ensuring privileges are assigned to its personnel.
7.2.3.	Rackspace maintains a default deny-all authorization model. Customer is responsible for implementing its own access control policy.
7.3.	Rackspace is responsible for developing security policies and procedures and ensuring adherence by all personnel. Customer is responsible for implementing its own access control policy.
8.1.	Section Header
8.1.1.	Rackspace to ensure all employees receive a unique ID before access is granted to Rackspace resources. Access to Customer PHI data environment by such employees to utilize a unique ID, or shall be identifiable to a unique ID. Customer to do the same for its employees.
8.1.2.	Rackspace is responsible for implementing policies and procedures to govern User ID authorizations and continuous validation. Customer to do the same.
8.1.3.	Rackspace to ensure employee access is immediately revoked following termination. Rackspace is responsible for revoking accounts for Customer terminated employees upon request and approval. Customer to do the same for its terminated employees. Alternatively, Customer is responsible for immediately notifying Rackspace of terminated employees where Rackspace is the responsible party for revoking associated accounts.
8.1.4.	Rackspace to ensure internal user accounts for all Rackspace personnel are removed/disabled after 90 days of inactivity on Rackspace resources. Customer to do the same for its internal personnel. If Rackspace's DPAuth service is elected, Customer VPN users can be automatically disabled after 90 days of inactivity by Customer controlled configuration.
8.1.5.	Rackspace to ensure its vendor IDs are enabled only when needed, disabled when not in-use, and monitored. Customer to do the same when vendor IDs are created by Customer.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
8.1.6.	Rackspace will apply its hardening standard upon request and approval from Customer to enforce a lockout policy in accordance with the associated requirement. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
8.1.7.	Rackspace will apply its hardening standard upon request and approval from Customer to enforce a lockout policy in accordance with the associated requirement. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
8.1.8.	Rackspace will apply its hardening standard upon request and approval from Customer to enforce an idle session limit in accordance with the associated requirement. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
8.2.	Rackspace and Customer to employ at least one of the authentication methods in addition to assigning a unique ID (or a mechanism to uniquely identify administrators) to each employee.
8.2.1.	Rackspace to ensure strong cryptography is used to render all authentication credentials unreadable at rest and during transit for all transmission and storage mechanisms employed by Rackspace. Customer to do the same for all other cases.
8.2.2.	Rackspace is responsible for user identity validation for all Customer requests for Rackspace assistance.
8.2.3.	Rackspace will apply its hardening standard upon request and approval from Customer to enforce a passwords/phrase policy in accordance with the associated requirement. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
8.2.4.	Rackspace will apply its hardening standard upon request and approval from Customer to enforce a password/passphrases expiration policy in accordance with the associated requirement. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
8.2.5.	Rackspace will apply its hardening standard upon request and approval from Customer to enforce a password history policy in accordance with the associated requirement. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
8.2.6.	Upon request and approval from the Customer, Rackspace will implement in accordance with the associated requirements. Customer to do the same for all other cases.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
8.3.	Rackspace is responsible for incorporating 2-factor authentication for its employees that have a business need to access Rackspace's secure management systems with network access to Customer resources. If Rackspace's optional Secure Cloud Access service is elected, Customer access to its network will also leverage 2-factor authentication. Note: Direct Connect and VPN are considered local network access.
8.4.	Rackspace to ensure personnel awareness of security authentication policies and procedures. Customer is responsible for implementing its own organizational security policies.
8.5.	Rackspace to ensure generic/shared user IDs are disabled or removed on all Rackspace resources, unless accountability can be assigned to such user ID. Additionally, such generic/user IDs, if in use on Customer systems within the PHI environment, have other mechanisms to allow for actions taken with such shared IDs to be associated with a unique ID on an external system. Customer to do the same.
8.5.1.	Rackspace is responsible for ensuring remote access by its employees to Customer solutions require unique authentication credentials per customer.
8.6.	If Rackspace's optional 2-Factor Authentication service is elected, individual logical tokens and PIN numbers are leveraged for all authorized Customer remote access VPN users. Rackspace to do the same for 2-factor access to its network.
8.7.	Rackspace is responsible for meeting this requirement for its employees which may need to incidentally access PHI in databases, as well as for any applications or processes implemented by Rackspace (i.e. database backups) which may need programmatic access to the databases containing PHI. Customer is responsible for the same for any Customer employee or applications.
8.8.	Rackspace is responsible for developing security policies and procedures and ensuring in use and disseminated to all personnel. Customer is responsible for implementing its own organizational security policies.
9.1.	Rackspace is responsible for this requirement within its facilities.
9.1.1.	Rackspace is responsible for this requirement within its facilities.
9.1.2.	Rackspace is responsible for this requirement within its facilities.
9.1.3.	Rackspace is responsible for this requirement within its facilities.
9.2.	Rackspace is responsible for this requirement within its facilities.
9.3.	Rackspace is responsible for this requirement within its facilities.
9.4.	Section Header
9.4.1.	Rackspace is responsible for this requirement within its facilities.
9.4.2.	Rackspace is responsible for this requirement within its facilities.
9.4.3.	Rackspace is responsible for this requirement within its facilities.
9.4.4.	Rackspace is responsible for this requirement within its facilities.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
9.5.	Responsibility of Rackspace and Customer (if applicable) to ensure all media is physically secured.
9.5.1.	Responsibility of Rackspace and Customer (if applicable) to ensure media backups are secured.
9.6.	Section Header
9.6.1.	Responsibility of Rackspace and Customer (if applicable)t to classify all media
9.6.2.	Responsibility of Rackspace and Customer (if applicable) to ensure media is sent in accordance to the requirement.
9.6.3.	Responsibility of Rackspace and Customer (if applicable) to ensure management approval.
9.7.	Section Header
9.7.1.	Responsibility of Rackspace and Customer (if applicable) to ensure properly maintained inventory logs.
9.8.	Section Header
9.8.1.	Customer is responsible for ensuring hard-copy materials with PHI data can't be reconstructed.
9.8.2.	Responsibility of Rackspace and Customer (if applicable) to ensure PHI data on electronic media is rendered unrecoverable.
9.9.	Not Applicable to HIPAA environments.
9.9.1.	Not Applicable to HIPAA environments.
9.9.2.	Not Applicable to HIPAA environments.
9.9.3.	Not Applicable to HIPAA environments.
9.10.	Responsibility of Rackspace and Customer to ensure security policies and procedures for restricting physical access.
10.1.	Rackspace is responsible for ensuring its access control system provides user accountability for its employees on all supported system components. Customer is responsible for the same.
10.2.	Section Header
10.2.1.	Rackspace is responsible for logging individual access to PHI data on all systems leveraging Rackspace's optional encryption services. Customer is responsible for logging individual user access to PHI data on all system components outside of Rackspace's services.
10.2.2.	Rackspace ensures recording of all actions taken by any individual with administrative privileges for any audit trail written to Rackspace's Event Management service with such action information. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service.
10.2.3.	Rackspace ensures access to audit trails is logged on system components logging to Rackspace's Event Management service. Customer is responsible for this requirement for all system components not logging to Rackspace's Event Management service.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
10.2.4.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure invalid logical access attempts are logged for supported operating systems. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for ensuring invalid logical access attempts are logged on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
10.2.5.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure the use of identification and authentication mechanisms are logged. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for logging mechanisms on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
10.2.6.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure initialization, stopping, and pausing of audit logs are logged. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
10.2.7.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure the creation and deletion of system-level objects are logged. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
10.3.	Section Header
10.3.1.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure user identification is included in log entries. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
10.3.2	Rackspace will apply its hardening standard upon request and approval from Customer to ensure the type of event is included in log entries. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
10.3.3.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure the date and time is included in log entries. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.
10.3.4.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure success and failure indication is included in log entries. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace or that do not have Rackspace's Continuous Audit service.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
10.3.5.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure the origination of event is included in log entries. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace that do not have Rackspace's Continuous Audit service.
10.3.6.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure the identity or name of affected data, system component, or resource is included in log entries. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace that do not have Rackspace's Continuous Audit service.
10.4.	Upon request, all supported system components will receive NTP configurations for time synchronization. Customer is responsible for the same on all system components not configured and/or supported by Rackspace.
10.4.1.	Rackspace will ensure its central time server receives time from designated highly available external sources. Customer is responsible for the same on all system components not configured and/or supported by Rackspace
10.4.2.	Rackspace will apply its hardening standard upon request and approval from Customer to ensure changes to time settings on supported system components are logged. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for ensuring the same on all system components not configured by Rackspace and/or that do not have Rackspace's Continuous Audit service.
10.4.3.	Rackspace is responsible for ensuring its time server only receives time updates from industry-accepted time sources. Customer to do the same as may be applicable.
10.5.	Rackspace is responsible for securing audit trails that are written to Rackspace's optional Event Management service. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service. Section Header
10.5.1.	Rackspace is responsible for protecting audit trails that are written to Rackspace's optional Event Management service. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service.
10.5.2.	Rackspace is responsible for protecting audit trails that are written to Rackspace's optional Event Management service. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service.
10.5.3.	Rackspace is responsible for backing up audit trail files that are written to Rackspace's optional Event Management service. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service.
10.5.4.	Rackspace to ensure all logs written to Rackspace's optional Event Management service will be secured and centralized. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
10.5.5.	Rackspace is responsible for leveraging file-integrity monitoring on existing log data written to Rackspace's optional Event Management service. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service.
10.6.	Section Header
10.6.1.	Rackspace is responsible for performing daily log review on supported log data written to Rackspace's optional Event Management service. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service, and unsupported log data.
10.6.2.	Rackspace is responsible for performing daily log review on supported log data written to Rackspace's optional Event Management service. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service, and unsupported log data.
10.6.3.	Rackspace is responsible for following up on anomalies identified during daily log review of supported log data written to Rackspace's optional Event Management service. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service, and unsupported log data.
10.7.	Rackspace will ensure audit trails written to Rackspace's optional Event Management service are retained for at least one year. Customer is responsible for this requirement on all system components not logging to Rackspace's Event Management service.
10.8.	Rackspace to ensure personnel awareness of organizational security policies and procedures for monitoring all access to network resources. Customer is responsible for implementing their own organizational security policies.
11.1.	Rackspace is responsible for this control within its facilities.
11.1.1.	Rackspace is responsible for this control within its facilities.
11.1.2.	Rackspace is responsible for this control within its facilities.
11.2.	Section Header
11.2.1.	Rackspace will configure recurring monthly internal scans against the system components leveraging Rackspace's optional Vulnerability Assessment service. Customer to do the same on all other system components not scanned by this optional service.
11.2.2.	Upon request, Rackspace will configure recurring monthly external scans leveraging Rackspace's optional Intrusion Detection Service. Customer to do the same on all other system components not scanned by this optional service.
11.2.3.	Rackspace will configure recurring monthly scans meeting the internal scan requirement against the system components with the optional service. Customer to determine rescan necessity and perform on-demand external scanning as needed. Customer to also scan other system components not leveraging optional Rackspace scanning services.
11.3.	Customer is responsible for implementing a methodology for the penetration testing of its networks.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
11.3.1.	Customer is responsible for performing external penetration testing against its networks.
11.3.2.	Customer is responsible for performing internal penetration testing against its networks.
11.3.3.	Customer is responsible for correcting exploitable vulnerabilities detected during penetration tests in accordance with the requirement.
11.3.4.	Customer is responsible for performing penetration testing against its networks at least annually and after any change to segmentation controls/methods.
11.4.	Rackspace's optional Intrusion Detection service will monitor and alert in accordance with the associated requirements for all system components with the IDS agent installed. Customer to request and approve IDS agent deployment. Customer to do the same on all system components not leveraging Rackspace's Intrusion Detection service.
11.5.	If Rackspace's Continuous Audit service is elected, Rackspace will deploy file integrity monitoring software for supported operating systems in accordance with the associated requirements. Customer is responsible for requesting and approving such software. Customer is responsible for the same on all system components not leveraging Rackspace's Continuous Audit service, and unsupported operating systems. Customer is responsible for identifying configuration and content files for critical Customer content (excluding OS).
11.5.1.	Customer to implement a process to respond to alerts generated by Rackspace's Continuous Audit service if elected. Rackspace to only investigate change if requested by Customer.
11.6.	Rackspace is responsible for implementing security policies and procedures for security monitoring and testing. Customer is responsible for implementing their own set of organizational policies.
12.1.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.1.1.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.2.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.3.	Section Header
12.3.1.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.3.2.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.3.3.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.3.4.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
12.3.5.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.3.6.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.3.7.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.3.8.	Rackspace will apply its hardening standard upon request and approval from Customer to enforce an automatic disconnect policy for RDP and SSH sessions in accordance with the associated requirement. In addition, if Rackspace's Continuous Audit service is elected, Rackspace will alert on any hardening deviations of this policy. Customer is responsible for the same on all system components not configured by Rackspace, using remote access technologies other than RDP and SSH, or that do not have Rackspace's Continuous Audit service.
12.3.9.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.3.10.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.4.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.5.	Section Header
12.5.1.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.5.2.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.5.3.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.5.4.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.5.5.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.6.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.6.1.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.6.2.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.

RESPONSIBILITY BREAKDOWN	
Requirement Number ("Requirement")	**Requirement Breakdown**
12.7.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.8.	Section Header
12.8.1.	Customer is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.8.2.	Customer and Rackspace are responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.8.3.	Customer is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.8.4.	Not Applicable
12.8.5.	Customer is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.9.	Rackspace and Rackspace are responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.10.	Section Header
12.10.1.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.10.2.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.10.3.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.10.4.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.10.5.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.
12.10.6.	Each party is responsible for meeting this security policy requirement to govern its internal policies and practices as it relates to security principles and protection of PHI data.

This HIPAA Business Associate Agreement (this "**HIPAA Agreement**") defines the rights and responsibilities of Customer and Business Associate with respect to Protected Health Information as defined in the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder, as each may be amended from time to time (collectively, "**HIPAA**"). This HIPAA Agreement is intended to satisfy any applicable obligations of Customer under 45 C.F.R. Sections 164.308(b), 164.314(a) and 164.504(e).

1. DEFINED TERMS.
For the purposes of this HIPAA Agreement, capitalized terms shall have the following meanings:

"**Agreement**" shall mean, collectively, the GSA and the HIPAA Agreement.

"**Business Associate**" shall mean Rackspace US, Inc., d/b/a Rackspace or such other entity as may be designated as the service provider in the GSA.

"**CFR**" shall mean the Code of Federal Regulations.

"**Customer**" shall mean the customer who is a party to the Service Order into which this HIPAA Agreement is incorporated.

"**Effective Date**" shall mean the date of Service Order into which this HIPAA Agreement is incorporated.

"**HIPAA Responsibility Matrix**" shall mean Exhibit A to the HIPAA Services Schedule.

"**Individual**" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

"**GSA**" shall mean that certain Global Services Agreement between Customer and Business Associate, together with any associated Service Schedules and Service Orders (which may also be referred to as Order Forms).

"**Privacy Rule**" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E, as may be amended from time to time.

"**Protected Health Information**" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information received by Business Associate from or on behalf of Customer.

"**Required By Law**" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

"**Secretary**" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

"**Security Rule**" shall mean the Standards for Security of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and C, as may be amended from time to time.

"**Security Standards**" shall mean those regulations relating to the security of electronic PHI at 45 C.F.R parts 160, 162, and 164, as may be amended from time to time.

Capitalized terms referenced in this HIPAA Agreement but not defined in this Section 1 shall have the meanings ascribed to such terms in the GSA.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

2.1. Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this HIPAA Agreement or as permitted or Required by Law.

2.2. Business Associate agrees to provide certain physical safeguards and administrative controls together with those Security Services elected by Customer and more specifically set forth in the GSA.

2.3. Business Associate shall have responsibility for those items specifically delineated in the HIPAA Responsibility Matrix and as may be appropriate for a Business Associate engaged in the provision of managed hosting services.

2.4. Business Associate agrees to mitigate, to the extent reasonably practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate or its agents or subcontractors in violation of the requirements of this HIPAA Agreement.

2.5. Business Associate agrees, in accordance with its HIPAA obligations associated with breach notification, to report to Customer any impermissible acquisition, access, use or disclosure of Protected Health Information of which it becomes aware promptly and without unreasonable delay, and in no case later than ten (10) business days after discovery of the acquisition, access, use or disclosure.

2.6. Business Associate agrees to require any agent, including subcontractors who are acting as business associates of the Business Associate and to whom it knowingly provides Protected Health Information, to adhere to the same restrictions and conditions that apply to Business Associate under this HIPAA Agreement with respect to such information.

2.7. All Protected Health Information maintained by Business Associate for Customer will be available to Customer in a time and manner that reasonably allows Customer to comply with the requirements under 45 CFR § 164.524. Business Associate shall not be obligated to provide any such information directly to any Individual or person other than to Customer.

2.8. All Protected Health Information and other information maintained by Business Associate for Customer will be available to Customer in a time and manner that reasonably allows Customer to comply with the requirements under 45 CFR § 164.526.

2.9. Business Associate agrees to make internal practices, books, and records available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary's determining Customer's compliance with the Privacy Rule and Security Standards.

2.10. In accordance with the applicable regulations, Business Associate is not required by this HIPAA Agreement nor Required By Law to make disclosures of Protected Health Information to Individuals and other persons or entities other than Customer. In the event that Business Associate is required to make a lawful disclosure, it shall document the disclosure as would be required for Customer to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR §164.528, and shall provide such documentation to Customer promptly upon request.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE.

Except as otherwise limited in this HIPAA Agreement or the GSA, Business Associate may access or maintain Protected Health Information to perform functions, activities, or services for, or on behalf of, Customer as specified in the Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Customer.

4. SPECIFIC USE AND DISCLOSURE PROVISIONS.

Except as otherwise limited in this HIPAA agreement or other portion of the GSA, Business Associate may:

(a) Access or maintain Protected Health Information for the proper management and administration of Business Associate or to carry out its legal or contractual responsibilities;
(b) Disclose Protected Health Information for the proper management and administration of Business Associate, provided that disclosures are (i) Required By Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached; and
(c) Use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).

5. CUSTOMER OBLIGATIONS.

Customer shall notify Business Associate of:

(a) any limitations(s) in Customer's notice of privacy practices in accordance with 45 CFR § 164.520 to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information;
(b) any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information;
(c) any restriction to the use or disclosure of Protected Health Information that Customer has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information;
(d) any discontinued use of elected Security Services to satisfy requirements set forth by the Security Rule and Privacy Rule for Customer's collection, use or disclosure of Protected Health Information; and
(e) any failure by Customer to maintain safeguards which are necessary to satisfy requirements set forth by the Security Rule and Privacy Rule but which have not been elected by Customer under the GSA.

Customer agrees that it will not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Customer.

6. TERM AND TERMINATION

6.1. The term of this HIPAA Agreement shall commence as of the Effective Date and continue for the term of the GSA (or Service Order associated with the HIPAA Services Schedule) and following termination of the GSA (or Service Order associated with the HIPAA Services Schedule), until all Protected Health Information is either destroyed or returned to Customer or its designee.

6.2. Breach of this HIPAA Agreement shall constitute a material breach of the GSA giving rise to a right of termination (subject to the applicable right to cure).

6.3. No earlier than fourteen (14) days and no later than thirty (30) days following termination or expiration of the GSA (or Service Order associated with the HIPAA Services Schedule) for any reason, Business Associate shall destroy all Protected Health Information. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate as well as Business Associate itself. Business Associate shall retain no copies of the Protected Health Information, however Customer shall retain copies of the Protected Health Information following termination as may be Required By Law. In the event Business Associate determines that destroying the Protected Health Information is infeasible, Business Associate shall promptly provide Customer notification of the conditions that make return or destruction infeasible. Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the destruction infeasible, for so long as Business Associate maintains such Protected Health Information. Customer

shall bear the reasonable cost of storage of the Protected Health Information for as long as storage by Business Associate is required in the event the parties determine that destruction and/or return is infeasible.

7. MISCELLANEOUS.

7.1. AMENDMENT.

Business Associate and Customer agree to take such action as is reasonably necessary to amend this HIPAA Agreement from time to time as may be necessary for Customer to comply with the requirements of HIPAA; provided, however, that in the event HIPAA is amended or its implementing regulations are modified in such a manner that would require Business Associate to take any actions that would materially increase the cost of Business Associate providing service under the Agreement, the parties agree that Customer shall be responsible for the reasonable costs of any such actions or changes on a pro rata basis, or in the alternative, Business Associate shall have the option to terminate the Agreement on (60) sixty days advance written notice.

7.2. SURVIVAL.

The respective rights and obligations of the parties under this HIPAA Agreement shall survive the termination of the GSA.

7.3. INTERPRETATION.

Any ambiguity in the HIPAA Agreement shall be resolved to permit either the Business Associate or the Customer to comply with HIPAA and the Privacy Rule.

[END OF EXHIBIT B]