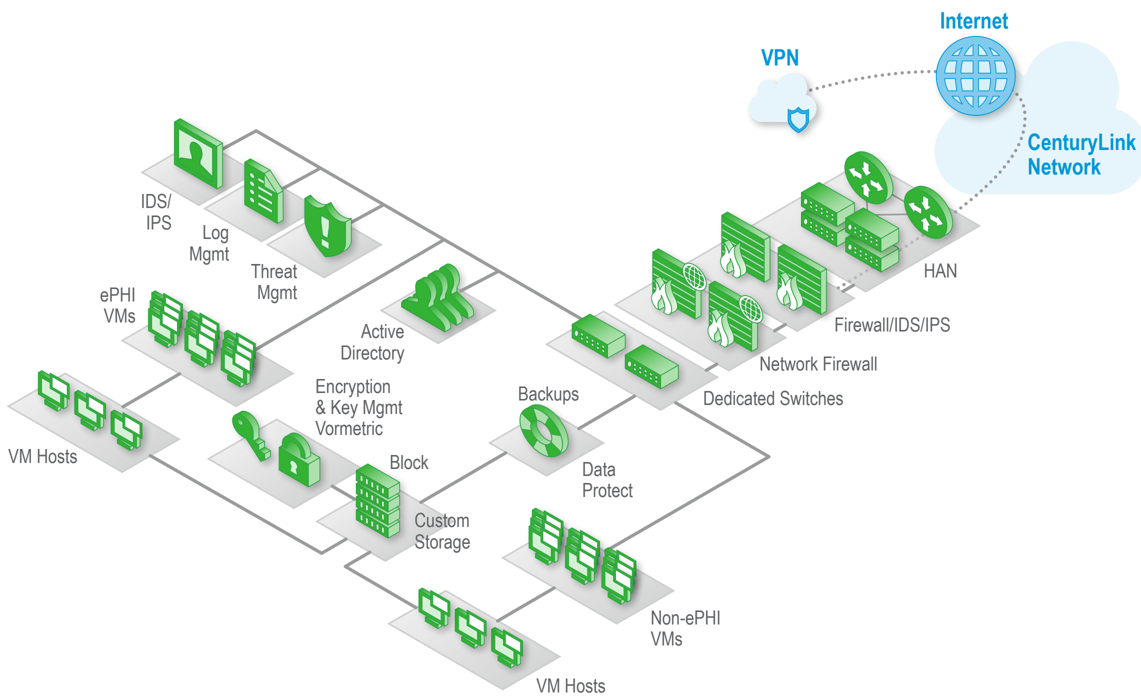
REFERENCE ARCHITECTURE

CenturyLink® Security: HIPAA / HITECH Compliance

CenturyLink achieves HIPAA compliance for your data through strict adherence to required guidelines, policies and procedures. These efforts include multiple firewalls and non-ePHI VMs as well as encryption and key management.



Covered entities and their business associates that are required to comply with the U.S. Health Insurance Portability and Accountability Act (HIPAA) can leverage CenturyLink to process, maintain, and store individually identifiable health information or protected health information (PHI). With the required controls in-place in the customer environment (data encryption, access restrictions, etc.). CenturyLink will sign a Business Associate Agreement (BAA) that can be leveraged as part of the customer's overall compliance program. If the protected data is encrypted and if the CenturyLink staff does not have access to it, a customer is not obligated to arrange a BAA to be in compliance with HIPAA.

Technical Specifications

Dedicated managed firewall service with intrusion detection & prevention

- Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. HIPAA 164.312(c)(1)

Data protect encrypted backup service

- Create a retrievable, exact copy of ePHI, when needed, before movement of equipment. HIPAA 164.310(d)(1)

Managed active directory service with custom rules

- Assign a unique and/or number for identifying and tracking user identity. HIPAA 164.312(a)(1)

Vormetric encryption and key management

- Implement a mechanism to encrypt and decrypt ePHI. HIPAA 164.312(a)(1)
- Implement security measures to help ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of. HIPAA 164.312(e)(1)

CenturyLink® Security: HIPAA / HITECH Compliance

Managed vpn with two-factor authentication

- Implement a mechanism to encrypt ePHI whenever deemed appropriate. HIPAA 164.312(e)(1)

Managed threat management security scanning and penetration testing

- Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. HIPAA 164.312(c)(1)

Integrity monitoring (Tripwire)

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. HIPAA 164.312(b)
- Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. HIPAA 164.312(c)(1)
- Implement a mechanism to encrypt ePHI whenever deemed appropriate. HIPAA 164.312(e)(1)

Managed intrusion detection & prevention (IDS/IPS)

- Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. HIPAA 164.312(c)(1)

Log management

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI. HIPAA 164.312(b)
- Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner. HIPAA 164.312(c)(1)
- Implement a mechanism to encrypt ePHI whenever deemed appropriate. HIPAA 164.312(e)(1)

Custom storage array (SAN)

- Implement a mechanism to encrypt and decrypt ePHI. HIPAA 164.312(a)

The CenturyLink Products and Services illustrated in this document are guidelines for implementing a HIPAA compliant solution using Dedicated Cloud. Attaining overall HIPAA compliance remains the responsibility of the Customer.

CenturyLink® Business