COUPA HEALTHCARECLOUD

COUPA HEALTHCARE CLOUD PROTECTS PRIVATE HEALTH INFORMATION IN FINANCIAL APPLICATIONS AS REQUIRED BY HIPAA

Coupa is committed to partnering with health insurers and care providers to deliver savings so urgently needed in the sector without sacrificing patient care outcomes or patient experiences. Under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, insurers and providers must take steps to protect Electronic Protected Health Information (ePHI) of their customers or patients. Coupa's Healthcare Cloud provides protections of ePHI required by HIPAA.

While Coupa does not provide any patient records management or patient care services, customers are protected in cases where ePHI is entered into Coupa by staff members. Coupa recommends against using ePHI such as Medical Record Numbers (MRNs) as part of business process or integration design. There are certain cases where ePHI may be entered in the context of a financial transaction. Examples include submitting an expense report for flowers with a patient's name in the expense description, attaching a receipt with the patient's name or room number, or attaching a laboratory report to an invoice. Coupa protects customers against the risk of exposure of ePHI.

Under HIPAA, insurers and providers who allow service providers to create, receive, maintain, or transmit ePHI on their behalf must enter into Business Associate agreements (BAA) with those providers. BAAs extend responsibility for protection of ePHI to those providers. Coupa's Healthcare Cloud lets Coupa enter into a Business Associate relationship with customers, ensuring that ePHI appropriately entered into Coupa for spend management is protected as mandated under HIPAA. Coupa has taken a number of steps to protect ePHI according to the standards set out by HIPAA including Administrative Safeguards, Physical Safeguards, and Technical Safeguards.

Technical Safeguards
Under Coupa's Healthcare Cloud, additional technical safeguards have been put in place to protect PHI. Rigorous access controls ensure that only appropriate parties have access to Coupa systems. Numerous controls within the Coupa technology and infrastructure ensure that data is secure both in transit and at rest.

Data in Transit
Coupa encrypts data in transit to ensure that any data that is intercepted while in transit is not compromised. Data is encrypted via SSL before being transferred between the server and the end user through web browser, mobile app, or email. Transfer of data between servers and storage within the Cloud for Healthcare is also encrypted. Coupa mail servers support enforced TLS to secure emails between Coupa and customer mail servers. Purchase orders and other data passed from Coupa to customer systems is encrypted using SFTP.

Data at Rest
Coupa employs multiple strategies for encrypting data at rest. Data entered entered in to ePHI designated fields such as descriptions, comments and specific custom fields in Coupa are encrypted on the client side prior to being saved in the database. File attachments are encrypted both on the client side prior to being saved, and again on the server side prior to being saved. The Coupa mobile app for iPhone is encrypted to protect data at rest on the iPhone device. Android OS supports encrypting the entire file system to protect data at rest on Android devices. Inbound and outbound emails are encrypted at rest in the email queue before being processed. Coupa decommissions disk storage using a secure wipe protocol commensurate with US Department of Defense standards.

Strong Encryption
Coupa uses strong encryption methods to ensure that ePHI is protected against compromise

- **Encryption algorithms -** Coupa uses PGP to encrypt file attachments and AES 256 to encrypt application data.
- **Key Management -** Coupa uses a key management service to manage encryption keys. Each Coupa customer is assigned unique encryption keys.

Physical Safeguards
Coupa uses Amazon's EC2 service to provide the computing capacity needed to run our financial applications and Amazon's S3 service to store file attachments. Amazon is a well known provider which has appropriate controls in place for facility security, access control, and contingency operations. In addition, Coupa employs security provisions for our own facilities including badge access control, workstation security, backups, and workstation reuse.

Administrative Safeguards
Coupa has implemented business policies and procedures to prevent loss of ePHI. Coupa's Director of Security and Compliance is responsible for the development and implementation of these policies and procedures. Access to systems that handle ePHI is only given to personnel after a credit and criminal background check. Personnel undergo HIPAA training prior to being granted access to systems containing ePHI. Termination procedures ensure that access is terminated appropriately. Security incident response and breach notification procedures ensure that any incidents are properly reported to supervisors, customers and regulatory authorities as required by law. Contingency plans ensure availability of data in case of a disaster.

Coupa's Business Associates
Organizations that may have access to ePHI as part of their business relationships with Coupa have signed BAAs with Coupa.