

IT Design and Security Processes

Overview

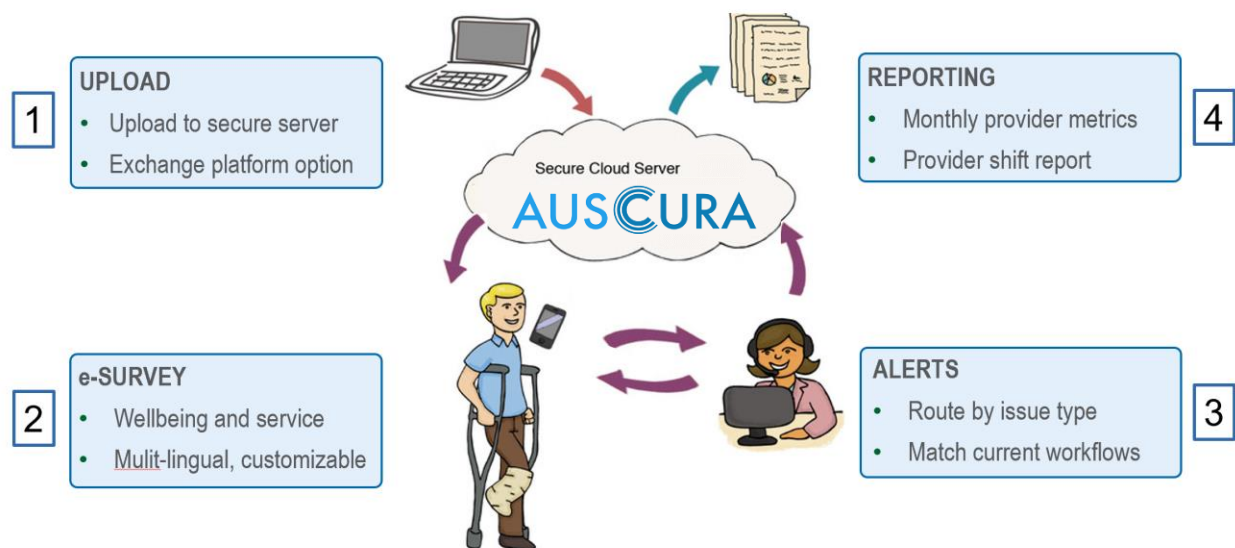
Auscura is a technology company that automates patient-provider communication using a platform of SaaS products. SmartContact™ reaches out to discharged patients using an SMS or email link to a survey that assesses wellbeing and experience.

Auscura complies with patient privacy and data security requirements defined by HIPAA and HITECH. Limited PHI including 10 required and 16 optional data fields are abstracted (see attached file describing data specifications) from the EMR.

For many applications, a scheduled daily feed from the client hospital's EHR is automatically and securely uploaded to the Auscura cloud server. All patients seen in the department the prior calendar day can be abstracted at about 6 am (allowing a 6-hour gap to ensure nearly all have a final disposition).

System Design

D



Data Security Features

- Hosted on the Microsoft Azure platform, an industry leader for availability and scalability, using single tenancy for each client
- Armor (<https://www.armor.com/>) is used for security threat protection with HITRUST and PCI DSS Level 1 certifications and third-party audits
- Strict authentication with extended validation certificates
- Role-based authorization and access control with multiple-layer passwords and audit trails
- OAuth-2 (Token based) authentication
- 256-bit SSL encryption encryption of PHI data at rest and during transmission
- Automated data backup and restore modules setup in different servers/regions for disaster recovery
- Secure FTP for data transfers and SSH for server access
- Automated deployments for continuous integration and delivery

IT Design and Security Processes

Network Diagram

