Summary

This document contains specific information about security safeguards and security breech protocols of HealthTech Solutions (HTS). All commercial products developed, produced, and distributed by HTS abide by the protocol in this document. Products will transfer and store the following sensitive information; Protected Health Information (PHI), Personally Identifiable Information (PII), company, and employee confidential information.

Updated: June 16, 2017

Contact: Eric Pahl, Security Officer, HTS
815-575-7017
HealthTech Solutions, Inc.
537 S Van Buren St.
Ste. A
Iowa City, IA 52240

Platforms: Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Apple Safari, Apple iOS, and Google Android.

Products: Organizer App, Organizer Admin, and TXP Chat.

I. HIPAA

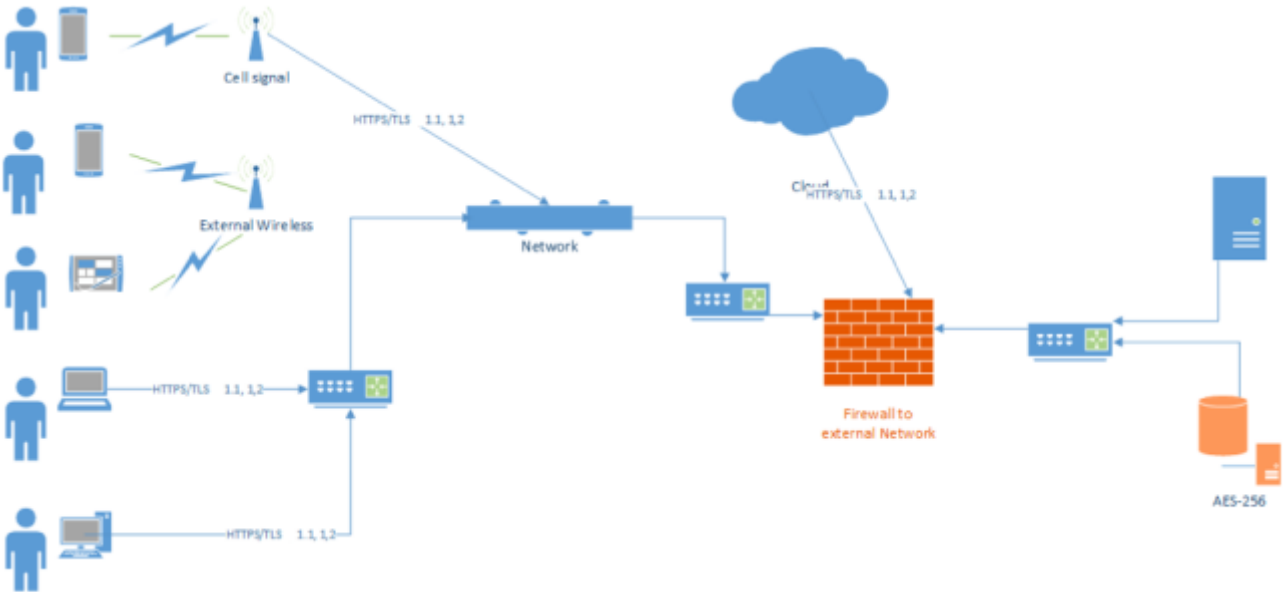
All interactions on any Products are recorded in the HIPAA Activity Audit Log - a log that captures access date/time, user account identifier, records accessed and privileged commands. Logs are retained for at least seven years. Local security administrators can generate reports from logs containing at least; user account identifier, user name, user security level, and user's last login date. The integrity of the audit trail is maintained for disabled or deactivated users and Products will record date/time when accounts have been compromised, disabled or deactivated.

II. HITECH

Products transfer and store electronic PHI through integrations with Electronic Health Record systems and by direct input from users as text, videos, or photos. Products are not considered EHR systems by HITECH.

III. Data Security

All data transferred and stored by Products reside within the United States. Data is encrypted in transit (HTTPS TLS 1.1 and 1.2) and in storage (AES 256) meeting NIST Special Publications 800-52 Rev1 and 800-111 standards. Data destruction/sanitation and storage reclamation processes are designed to prevent customer data form being exposed to unauthorized individuals. These processes follow techniques detailed in DoD 5220.22-M and NIST 800-88r1. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices. Each customer's data will be segregated from other customers through logical controls. Encrypted and signed claims based authorization tokens are used to prevent tampering and only allow access to data the user is permitted to see. Backend access is only by SSH and includes role-based controls to manage and audit admin/backend users.



HTS data centers are hosted by Amazon Web Services (AWS); Tier 3+, SSAE16 certified with SOC 1, 2, and 3 completed in April 2017. Each component within AWS data centers is tested and maintained regularly every 90 days. AWS provides several reports from third-party auditors who have verified compliance with a variety of computer security standards and regulations (aws.amazon.com/compliance). Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee. All physical accesses to data centers by employees are logged and audited routinely. Data center access lists are audited regularly, every 90 days by Amazon Web Services (AWS) and HTS.

Redundancy is built into the HTS databases and products offering customizable data archiving and retention. Customer data will be retained for the life of the customer contract, available from export at the termination of the contract, and then sanitized from HTS meeting guidelines from NIST SP 800-88 rev1. Disaster Recovery Plans (DRP) are on file for all HTS systems. DRPs are updated, reviewed and exercised on a regular basis, every 6 months, anytime a major change is made to BAA, and in response to any major hardware or software failure or destruction of facilities. Customer data will never be shared with third parties without permission from customer.

IV. Customer Contact and Authorization Policy

Available in separate appendix or by request.

V. Account Security

In order to access Products, unique login and password are required. Account and password criteria, expiration, auto-logoff, and other administrative policies/procedures are configurable by customers. Products support multiple levels of account access configurable by customers. Products are designed to be accessible and full-featured, HTS does not allow for multiple levels of access based on location unless customers ask specifically.

VI. User Training

All HTS Products can be accessed in a training sandbox without any PHI or security risk. Training is coordinated with HTS representatives and any Product updates will be accompanied by an opportunity for virtual and/or in-person training from a certified HTS support technician.

VII. Mobile Access

HTS Products are accessible via any of our certified Platforms. For native mobile application Products, a user is registered using a phone number and email. The phone number is verified by a pin number containing six pseudo-random numbers expiring in five minutes and delivered via SMS text message. Both the user and customer administrator are notified of successful registration. Password recovery is completed through an expiring (five minutes) secure email link, and within the native mobile application, by using a temporary pin number delivered via SMS, expiring in five minutes. Data is not stored locally or in cache on any Products, data is merely accessed by Products and displayed for the users. Data is transferred to/from the phone using HTTPS TLS v1.1 and v1.2. Native mobile applications allow for photo and video capture, and file upload.