TISSUE ANALYTICS
SIMPLIFYING WOUNDCARE

Secure Application Development Policy

Version: 1.0
Effective Date: 10/21/16

Author: Joshua Budman, Chief Technology Officer

Disclaimer: This policy was created by Tissue Analytics, Inc. for the sole use of its employees and clients.

Overview

Tissue Analytics, inc. (TA) is responsible for developing software that analyzes, stores and transmits protected health information (PHI). TA must adhere to stringent secure software development guidelines, outlined in this document, in order to ensure the safety of this sensitive data.

Purpose

The purpose of this policy is to establish standards for the secure development policy used by TA. Effective implementation of this policy will minimize the risk of sensitive data being accessed by potentially malicious actors.

Scope

All employees, contractors, consultants, temporary and other workers at TA and its subsidiaries must adhere to this policy. This policy applies to employees or contractors employed by TA.

Policy

4.1 General Requirements

4.1.1 Users' ability to access actions that can perform update, modification or deletion in the database must be password-protected

4.1.2 All stored data must be encrypted using AES-256 while at rest or in use
4.1.3 All data collected by the mobile device must be purged from the device when it is sent to TA's cloud in keeping with NIST standards for media sanitization
4.1.4 All data must be encrypted using TLS in transit
4.1.5 Detailed error messages must not be accessible to users
4.1.6 All user input and output must be validated
4.1.7 Any access to sensitive data, including viewing said data, requires authentication.
4.1.8 Each facility must have a separate database installation to prevent data contamination
4.1.9 Scope of user action must be role-based and roles must be set by the appointed facility software administrator
4.1.10 Memory and CPU usage must be monitored at all times using commercial-grade software
4.1.11 Logs must not contain user credentials
4.1.12 URLs must not contain session ID's
4.1.13 Auto-complete cannot be turned on for password fields unless requested by the client and approved by TA system administrators
4.1.14 Local filepaths must not be exposed

Policy Compliance

5.1 Compliance Measurement
The TA information security team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Information Security team in advance.

Related Standards, Policies and Processes

- Software Development Lifecycle Summary Diagram
- Password Protection Policy
- Password Construction Guidelines

Definitions and Terms

Revision History

Date of Change	Version Number	Responsible	Summary of Change