TISSUE ANALYTICS
SIMPLIFYING WOUNDCARE

Data Encryption Policy

Version: 1.0
Effective Date: 11/20/16

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

Encryption of data is essential when dealing with highly sensitive client data. Proper encryption will minimize the risk of data usable by unwanted or malicious third parties. Tissue Analytics, inc. (TA) puts a high priority on encryption of its data both at rest and in transit.

Purpose

The purpose of this policy is to establish standards for the data encryption practices of all TA-associated software. Effective implementation of this policy will minimize the risk of unintended or undesirable use of TA-collected PHI by unwanted or malicious 3rd parties.

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 All data stored on TA's servers is encrypted using 256-bit Advanced Encryption Standard (AES-256) at rest.

4.1.2 All data collected by the mobile device is encrypted on the device itself using AES-256 immediately after it is transmitted to TA's cloud. Immediately thereafter, said data is purged from the mobile device in keeping with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=50819.
4.1.2 Data is encrypted in transit using Transport Layer Security 1.x (TLS1.x).
4.1.3 As a result of the recent Padding Oracle On Downgraded Legacy Encryption ("POODLE") attack, TA avoids use of Secure Socket Layer 3.0 (SSL3.0) based encryption. Due to their risk of man in the middle attacks, TA also avoids the use of Diffie-Helman-Merkle (DHM) exchanges.
4.1.4 All authentication uses standard keyed Hash Method Authentication Code (HMAC) based algorithms.

Policy Compliance

5.1 Compliance Measurement

The Infosec 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 Infosec team in advance.

Related Standards, Policies and Processes

Definitions and Terms

Advanced Encryption Standard (AES): Specification of the encryption of electronic data defined by NIST in 2001.
National Institute of Standards and Technology (NIST): The federal agency that works with industry to develop and apply technology, measurements and standards.
Transport Layer Security (TLS): Protocol that ensures privacy between communicating applications and their users on the internet.

Secure Socket Layer (SSL): Standard technology for establishing an encrypted link between a web server and a browser.
Diffie-Helman-Merkle (DHM): A cryptosystem that allows to computers to share information across an insecure network based on a shared private key.
POODLE (Padding Oracle On Downgraded Legacy Encryption)
Attack: Man-in-the-middle exploit that takes advantage of Internet clients' use of SSL 3.0.
Hash Method Authentication Code (HMAC): A small piece of data that helps authenticate the nature of a message.

Revision History

Date of Change	Version Number	Responsible	Summary of Change