TISSUE ANALYTICS
SIMPLIFYING WOUNDCARE

# Privacy Policy

**Version:** 1.0
**Effective Date:** 11/18/16

**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

Maintaining robust privacy policies is crucial for any product that transfers and stores sensitive data. Ensuring that all physical and cloud-based devices associated with Tissue Analytics, Inc. (TA) since these are involved in the storage of patient protected health information (PHI).

## Purpose

The purpose of this policy is to establish standards for the base privacy related practices of all equipment and software that is owned by TA. Effective implementation of this policy will minimize unauthorized access or leakage of TA's proprietary information as well as any client-associated PHI.

## Scope

All employees, contractors, consultants, temporary and other workers at TA and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated or leased by TA or registered under a TA-owned internal network domain. It also applies to any TA employee's personal devices that are involved in the storage of PHI or other sensitive data.

**Policy**

4.1 General Requirements

4.1.1 All employees must go through an industry-accepted Health Insurance Portability and Accountability (HIPAA). training program before handling any PHI as an employee of Tissue Analytics, inc.

4.1.2 Only employees that require access to PHI for work-related purposes are granted access to PHI stored by TA. This access is granted on an individual basis by Information Security.

4.1.3 All TA employee personal devices, regardless of whether or not they store PHI, must be password protected using password standards as described in the *Password Policy.*

4.1.4 If an employee's employment at TA ends for any reason, all of this employee's credentials on any TA-related software are removed. Future access to PHI is only granted if this employee's employment at TA is resumed.

4.1.5 No TA employee is permitted to store PHI on personal devices.

4.1.6 All PHI operated by TA is stored on Virtual Private Clouds (VPC) on Amazon Web Services. This provides TA servers with a physical partition from other Amazon clients. See the *perimeter firewall policy* for more detail on this.

4.1.7 All client sites are provided with partitioned data schemas on TA's application. Client sites must be personally vetted and approved by Information Security before receiving access to the TA software. This is also discussed in the Web Application/Server Security Policy.

4.1.8 All patients must be notified of the intended use of the software and their data prior to use.

4.1.9 All users must be notified that TA maintains the software. TA does not outsource any software development.

4.1.10. TA hosts a backup server in a geographically separate location from its primary survivor to serve as disaster recovery. All code and PHI is backed up on TA's backup server immediately after it is produced. TA performs daily verification of proper storage and backup of PHI.

4.1.11 In the mobile component, all PHI, which includes images and metadata, is immediately encrypted then subsequently wiped from the device after it is transmitted to TA's servers. More on this procedure is described in the Data Encryption Policy.

4.1.11 Any privacy-related concerns may be directed to Joshua Budman (josh@tissue-analytics.com, Chief Technology Officer) or Jason Hihn (jason@tissue-analytics.com, Chief Information Security Officer)

## Policy Compliance

5.1 Compliance Measurement

The 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

- Password Policy
- Perimeter Firewall Policy
- Web Application/Server Security Policy
- Data Encryption Policy

## Definitions and Terms

**Amazon Web Services (AWS):** A collection of remote computing services that together make up a cloud computing platform, offered over the Internet by amazon.com.

**Virtual Private Cloud (VPC):** On-demand configurable pool of shared computing resources allocated with a cloud environment

## Revision History

| Date of Change | Version Number | Responsible | Summary of Change |
|---|---|---|---|
| | | | |
| | | | |