# Security Governance Policy

## 1. Introduction

329design Inc. (“SimpleSet") is committed to ensuring the confidentiality, privacy, integrity, and availability of all electronic protected health information (ePHI) it receives, maintains, processes and/or transmits on behalf of its Customers in compliance with PIPEDA, HIPAA and GDPR. As providers of compliant, hosted infrastructure used by healthcare providers, SimpleSet strives to maintain compliance, proactively address information security, mitigate risk for its Customers, and assure known breaches are completely and effectively communicated in a timely manner. The following documents address core policies used by SimpleSet to maintain compliance and assure the proper protections of infrastructure used to store, process, and transmit ePHI for SimpleSet Customers.

## 2. Purpose

This Information Security Policy has been established to ensure the business continuity of SimpleSet and to minimize the risk of damage by preventing security incidents and reducing their potential impact. It defines the technical, administrative, and physical controls and configurations that users and administrators are required to implement in order to ensure the confidentiality, integrity, and availability of the data environments owned and operated by SimpleSet. The goal of this policy is to guide and direct SimpleSet workforce members on how to defend its assets against internal, external, deliberate or accidental threats. Adherence to the policy and associated standards referenced herein is mandatory for all employees and incorporates elements involving defined processes, integration, culture, and infrastructure

management, and serves as the central security policy that all SimpleSet employees must be familiar with and have working knowledge thereof.

# 3. Scope

The policy requirements and restrictions defined in this policy shall apply to all SimpleSet personnel, locations and systems. The policy covers SimpleSet network systems which is composed of various hardware, software, communication equipment and other devices designed to assist SimpleSet and its customers in the creation, receipt, storage, processing, and transmission of data and information.

SimpleSet provides secure and compliant cloud-based software. This hosted software falls into the category of Software as a Service (SaaS). It is the responsibility of the Chief Security Officer and Chief Privacy Officer to maintain this policy and ensure the contents of the policy are continually monitored and enforced.

## 3.1 Software as a Service (SaaS)

329 design Inc. develops and maintains SimpleSet, a web application used by doctors, physical therapists and other health professionals to create and deploy therapeutic exercise programs to their patients, primarily for the purposes of rehabilitation. SimpleSet also provides the ability for video conferencing in the delivery of telerehabilitation. SimpleSet does not have insight or access into SaaS Customers and their End-User devices and, as such, does not have the ability to secure or manage risk associated with End-User device vulnerabilities and security weaknesses.  SimpleSet makes every effort to reduce the risk of unauthorized disclosure, access, and/or breach of SaaS Customer data through network (Firewalls, private networks, etc), server settings (encryption at rest and in transit, IDS, etc), and secure workstations

(Automatic Logoff, disk encryption, etc) . For more specifics, refer to section 5 - SimpleSet Organizational Concepts of this document.

# 4. Compliance Inheritance

SimpleSet provides a HIPAA-compliant Application for its Customers.

SimpleSet agrees to go through a HIPAA compliance audit by any national, 3rd party compliance firm, to validate and map organizational policies and technical settings to HIPAA rules. The Business Associate requesting the audit is responsible for any costs related to the audit. Any audit would include both AWS and Azure production systems.

SimpleSet signs business associate agreements (BAAs) and Data Protection Agreements (DPA's) with its Customers. These agreements outline SimpleSet obligations and Customer obligations, as well as liability in the case of a breach. In providing infrastructure and managing security configurations that are a part of the technology requirements that exist in HIPAA, the GDPR and PIPEDA legislations and HITRUST framework, as well as future compliance frameworks, SimpleSet manages various aspects of compliance for Customers using the SimpleSet application. The aspects of compliance that SimpleSet manages for Customers are inherited by Customers, and SimpleSet assumes the risk associated with those aspects of compliance. In doing so, SimpleSet helps Customers achieve and maintain compliance, as well as mitigates Customer risk.

Certain aspects of compliance cannot be inherited. Because of this, SimpleSet Customers, in order to achieve full compliance or HITRUST Certification, must implement certain organizational policies. These policies and aspects of compliance fall outside of the services and obligations of SimpleSet.

HIPPA Rules to SimpleSet Policies controls are mapped below:

| **Administrative Controls HIPAA Rule** | **SimpleSet Control** |
|---|---|
| Security Management Process - 164.308(a)(1)(i) | Risk Management Policy |
| Assigned Security Responsibility - 164.308(a)(2) | Roles and Responsibility Policy |
| Workforce Security - 164.308(a)(3)(i) | Employee Policies |
| Information Access Management - 164.308(a)(4)(i) | Access Management Policy |
| Security Awareness and Training - 164.308(a)(5)(i) | Employee Policy<br>Training and Awareness Policy |
| Security Incident Procedures - 164.308(a)(6)(i) | Incident Response Policy<br>Vulnerability Management Policy |
| Contingency Plan - 164.308(a)(7)(i) | Disaster Recovery and Business Continuity Policy |
| Evaluation - 164.308(a)(8) | Auditing, Logging and Monitoring Policy |

| **Physical Safeguards HIPAA Rule** | **SimpleSet Control** |
|---|---|
| Facility Access Controls - 164.310(a)(1) | Access Management Policy<br>Disaster Recovery and Business Continuity Policy |
| Workstation Use - 164.310(b) | System Access Management Policy<br>Approved Tools Policy<br>Employee Policy |

| | |
|---|---|
| Workstation Security - 164.310('c') | Access Management Policy<br>Approved Tools Policy<br>Employee Policy |
| Device and Media Controls - 164.310(d)(1) | Removable Media and Media Destruction Policy<br>Data Management and Encryption Policy |

| **Technical Safeguards HIPAA Rule** | **SimpleSet Control** |
|---|---|
| Access Control - 164.312(a)(1) | Access Management Policy |
| Audit Controls - 164.312(b) | Auditing, Logging and Monitoring Policy |
| Integrity - 164.312('c')(1) | Access Management Policy<br>Auditing, Logging and Monitoring Policy<br>Vulnerability Management Policy |
| Person or Entity Authentication - 164.312(d) | Access Management Policy |
| Transmission Security - 164.312(e)(1) | Access Management Policy<br>Data Integrity and Encryption Policy |

| **Organizational Requirements HIPAA Rule** | **SimpleSet Control** |
|---|---|
| Business Associate Contracts or Other Arrangements - 164.314(a)(1)(i) | Business Associate Agreements and - Third Party Vendor and Due Diligence Policy |

| **Policies and Procedures and Documentation Requirements HIPAA Rule** | **SimpleSet Control** |
|---|---|
| Policies and Procedures - 164.316(a) | Policy Management Policy |

| | |
|---|---|
| Documentation - 164.316(b)(1)(i) | Policy Management Policy |

| **HITECH Act - Security Provisions HIPAA Rule** | **SimpleSet Control** |
|---|---|
| Notification in the Case of Breach - 13402(a) and (b) | HIPAA Breach Policy<br>Incident Response Policy |
| Timelines of Notification - 13402(d)(1) | HIPAA Breach Policy<br>Incident Response Policy |
| Content of Notification - 13402(f)(1) | HIPAA Breach Policy<br>Incident Response Policy |

# 5. SimpleSet Organizational Concepts

The physical infrastructure environment is hosted at Amazon Web Services (AWS) and Microsoft Azure. Azure is used as the backup site for the IT business continuity plan while the remaining infrastructure is contained within AWS's Canadian Region. AWS and Azure infrastructures and managed by AWS and Microsoft (respectively). SimpleSet does not have physical access into the network and system components of managed services offered by AWS and Azure. The SimpleSet environment consists of Nginx web servers, NodeJS application servers, MySQL database servers, Amazon Linux virtual servers as well as many of their managed service offering (ELB, CodePipeline, Elastic Beanstalk, CloudFront, S3, System Manager, Config, GuardDuty, CloudWatch, etc), ConfigServerFirewall (HIDS).

Within the SimpleSet Platform on AWS, all data transmission is encrypted and data at rest is also encrypted; this applies to all systems and managed services.  SimpleSet assumes all data

may contain ePHI, even though our Risk Assessment does not indicate this is the case, and provides appropriate protections based on that assumption.

It is the responsibility of the Customer to restrict, secure, and assure the privacy of all ePHI data at the Customer Device Level as well as educate the End-User regarding the use of the application and best practices for security and privacy at an End-User Device Level, as this is not under the control or purview of SimpleSet.

There is data and network segmentation in place in the SimpleSet Platform. The result of segmentation strategies employed by SimpleSet effectively create RFC 1918, or dedicated, private segmented and separated networks and IP spaces, for environments.

Additionally, Security Groups are used on each system for logical segmentation. The Security Groups are configured to restrict access to only justified ports and protocols. SimpleSet has implemented strict logical access controls so that only authorized personnel are given access to the internal management servers.

The load-balancer hosts are the only production systems that are externally facing and accessible via the Internet. The Nginx web servers and NodeJS application servers are not externally facing and can only be accessed directly using the Session Manager feature of the System Manager AWS service. The database servers are located on the internal AWS network and can only be accessed over an SQL connection. The access to the internal database is restricted to a limited number of personnel and strictly controlled to only those personnel with a business-justified reason. Remote access to the internal servers is not accessible except through the bastion host.

In the case of Telehealth, SimpleSet makes a reasonable attempt to establish a point to point connection between participants in order to reduce exposure of ePHI.  When point to point connectivity is not possible, AWS Kinesis Video Stream (TURN) is used to transport the encrypted stream between the participants of the Telehealth session.

All software and operating systems are tested end-to-end for usability, security and impact prior to deployment to production.

## 5.1 Internal Compliance

Violations of this standard and its procedures by employees may result in disciplinary action, up to and including termination of employment. Violation of this standard and procedures by others, including business associates and workforce members may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and provincial laws and regulations. SimpleSet reserves the right to notify law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

SimpleSet does not consider conduct in violation of this policy to be within a workforce member’s, business associate’s, or partner’s course and scope of employment or partnership, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, SimpleSet reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

If an employee, workforce member, business associate, or partner believes he or she has been requested to undertake an activity which he or she believes is in violation of this policy, he or she must provide a written or verbal complaint to the Security Officer or any manager as soon as possible.

# 6. Requesting Audit and Compliance Reports

SimpleSet, at its sole discretion, shares audit reports as available and Corrective Action Plans (CAPs), with customers on a case by case basis.  All audit reports are shared under explicit NDA between SimpleSet and the party to receive materials. Audit reports can be requested by SimpleSet workforce members for Customers or directly by SimpleSet Customers.

The following process is used to request audit reports:

1. Use the following link and fill out a request:  https://forms.gle/v59HMgupQn95EyfA7
2. The security or privacy officer will follow up by email in the next 10 business days.

SimpleSet handles the requests internally according to #SOP01 - Handling of Audit Reports Requests.

# 7. Version Control

SimpleSet maintains document versions using its Compliance Management System, Eramba. SimpleSet maintains documentation of its Standard Operating Procedures in Process Street.

Policies were last updated January 6, 2023.