RegenMed

InCytes™ DATA BREACH POLICY

Introduction

RegenMed provides Licensees with data processing services, including the ability to enter, store and access Personal Information about themselves and their Patients. RegenMed uses Amazon Web Services "AWS" as a sub-processor to store, pseudonymize and encrypt Personal Information. Data breaches are an unfortunate problem affecting organizations of all sizes and are equally varied in type, format, and severity. This policy, which incorporates the AWS Service Terms, describes RegenMed's role, responsibilities, and capabilities in helping its Licensee's prevent, identify and report data breaches.

Definitions

As defined within the inCytes™ License Agreement.

Roles

The inCytes™ Security Team comprises:

- Data Protection Officer: Alyssa Johncola – ajohncola@rgnmed.com
- Senior Developer: Dolph Courchaine – dcourchaine@rgnmed.com
- Senior Project Manager: William Graupmann – wgraupmann@rgnmed.com

The inCytes™ Security Team is responsible for the design, implementation and adjustments to this policy over time, including:

- Reviewing all reported potential data breaches.
- Reporting of all confirmed data breaches to the relevant Client and/or Licensee.
- Overseeing training and regular review of existing technical, organizational and procedural safeguards to prevent data breaches.

Technical and Organizational Security Methods

As described in the AWS Service Terms, and further detailed within the GDPR Addendum, AWS has implemented numerous technical and organizational methods to secure Personal Information processing. RegenMed's use of AWS as a subprocessor incorporates these measures into its own application, including:

- security of the AWS Network as set out in Section 1.1 of the AWS Security Standards;
- physical security of the facilities as set out in Section 1.2 of the AWS Security Standards;

- measures to control access rights for AWS employees and contractors in relation to the AWS Network as set out in Section 1.1 of the AWS Security Standards;

- processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by AWS as described in Section 2 of the AWS Security Standards.

In addition, RegenMed has elected to implement numerous additional security measures to support further Personal Information processing protection within its Architecture, including:

- pseudonymization and encryption to ensure an appropriate level of security; including:

  1. Bifurcation and region-selected independent storage of Personally Identifiable Information using the AWS Cognito Services;

  2. Pseudonymization of all Personal Information using AWS Cognito Services;

  3. Ability to revoke/restore account access at the request of verified License;

  4. Encryption of all servers storing Personal Information.

- measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services that are being operated by the Customer; including:

  1. Use of Amazon Elastic Container Service to provide failover copies;

  2. AWS access keys limited to inCytes™ Security Team;

  3. Automated, isolated deployment processes without inCytes™ Security Team, or any other users, access to Personal Information

- measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Personal Information in a timely manner in the event of a physical or technical incident; including:

  1. Automated backups of all Licensee Personal Information up to 7 days stored on separate, encrypted servers.

- processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer, including:

  1. Weekly technical calls among the inCytes™ Security Team, in which API logs are submitted and reviewed.

Data Breaches

Data breaches may still occur and can be caused by a number of possible, unpredictable, and/or uncontrollable factors, including:

Human Error

1. Loss of device with an open session;
2. Disclosure of Personal Information through unauthorized channels;
3. Sharing Login information with the wrong recipient;
4. Exporting Personal Information and improperly handling exported version;
5. Improper disposal.

Malicious Activity

1. Hacking and brute force entry;
2. Theft of devices with open sessions;
3. Scams which phish for login information or Personal Information.

Server/Computer Error

1. Application Bugs;
2. Failure of Cloud Services, including authentication, data entry, or reporting;
3. Loss of internet.

Data Breach Reporting

Data Breaches observed by AWS are obligated, under the AWS Service Terms, to be reported to the inCytes™ Security Team without undue delay.

Data Breaches observed by RegenMed Staff, Licensees, or other external parties are collected via email at security@rgnmed.com.

InCytes™ Security Team will notify the Client of a Data Breach without undue delay after becoming aware of the Data Breach, and provide the following if known:

1. The nature and type of the Data Breach breach;
2. The Personal Information and Licensees affected;
3. The suspected cause or source of the breach;
4. Information on whether or not the breach has been rectified;
5. Information on how the Client or Licensee can prevent further damages;
6. The contact information for the inCytes™ Security Team Member Liaison.

InCytes™ Security Team, at the written request of the Client, takes reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Information breach, including:

- Revoke access to the affected Licensee(s) preventing further unauthorized access;
- Establish whether lost or corrupted data can be restored, such as from our 7-day backups;
- Reset passwords for affected Licensee(s);
- Isolate and remove additional unauthorized access points.

InCytes™ Security Team will assist the Customer in relation to any personal Data Breach notifications Customer is required to make under the GDPR, RegenMed will include in the notification any such information about the Data Breach as RegenMed is reasonably able to disclose to the Customer, taking into account the nature of the Master Services Agreement, the information available to RegenMed, and any restrictions on disclosing the information, such as confidentiality.