RegenMed

InCytes™ PERSONAL DATA ARCHITECTURE

Overview

inCytes™ is a software as a service technology, built upon Amazon Web Services "AWS", which process large amounts of data, including health data and personally identifiable information. Such data, depending upon country, institution, and other policies, are often regarded as sensitive data, data concerning health, protected health information or PHI, personal data, or other similar terms. For purposes of this document, we will use terms and defined roles from the Global Data Protection Regulation, or GDPR.

In all instances, inCytes™ and Amazon Web Services shall serve as Data Processors, processing Personal Data according to the instructions by Data Controllers. This document helps inform Data Controllers of the existing infrastructure upon which inCytes™ is built, and of the available options for data processing. It is the Data Controller's obligation to select processing which complies with their local regulations and data governance policies.

Core Definitions:

- Data Controllers

Data Controllers are defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…"

- Personal Data

Personal Data is defined by the GDPR as "any information relating to an identified or identifiable natural person "data subject…". For the purposes of this document, Data Subjects shall be Patients.

- Personally Identifiable Information "PII"

All identifying information which alone or in aggregate identifies a natural person. Examples include names, contact information, addresses, etc.

- Pseudonymization

Pseudonymization is defined as "processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information." The GDPR further elaborates in Recital 26 "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

inCytes™ Server Architecture

- Subscriber Personal Data Entry

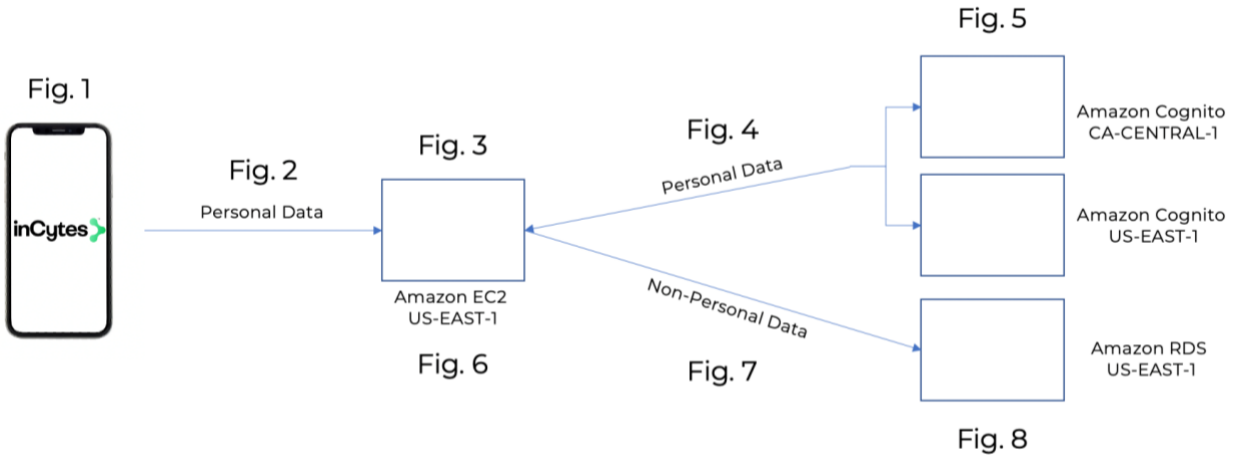

Fig. 1:

- Subscriber registers with email address;
- Subscriber creates 8-digit password, with minimum of one uppercase letter, one lowercase letter and one number;
- Subscriber chooses region where they would like to store Personal Data: USA or CA (Canada);
- Subscriber reads and signs Terms and Conditions;
- Once registered, Subscriber may elect to enable 2 Factor Authentication, requiring linking their mobile phone.

Fig. 2:

- Personal data, often including data concerning health, is entered through the authenticated account in the following ways:
    - Subscriber creates a Case, and manually registers a patient;
    - Subscriber creates a Case, and the Patient manually registers themselves through Benchmarc™;
    - Subscriber, their Delegate and/or the Patient complete Surveys.
- Personal data is sent through encrypted HTTPs.

Fig. 3:

- Personal data arrives at the Amazon EC2 Instance located in N. Virginia (US-EAST-1)

- All PII is identified according to:
    - Preset fields within the patient registration form, including Email, First Name, Middle Name, Last Name, Mobile Phone, Date of Birth and Country;
    - Manually designated questions within Surveys, for example, "Upload an image of X" or "Patient's Identification Number".

Fig. 4:

- Identified PII is transmitted to the Amazon Cognito Server location of Subscriber's choice:
    - N. Virginia (US-EAST-1) for USA;
    - Canada (CA-CENTRAL-1) for Canada.

Fig. 5:

- Amazon Cognito supports multi-factor authentication and encryption of data-at-rest and in-transit. Amazon Cognito is HIPAA eligible and PCI DSS, SOC, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant. Third-party auditors assess the security and compliance of Amazon Cognito as part of multiple AWS compliance programs.
- Amazon Cognito receives and stores all PII, and reverts an alphanumeric Subject ID (01caa87b-2b59-416c-b1a2-c5510f6555af) and Authentication Token, available exclusively to that Subscriber.
- The PII is stored with the following security measures:
    - Compliance validation and penetration testing;
    - Encryption for AWS Cognito;
    - Bit Keys.
- The Subject ID and Authentication Token is then sent back to the Amazon EC2 Instance located in N. Virginia (US-EAST-1).

Fig. 6:

- The Amazon EC2 Instance then pairs the Subject ID with the remaining de-identified data.

Fig. 7:

- The remaining data, which isnow pseudonymized and non-personal data, is transmitted to the Amazon RDS located in N.Virginia (US-EAST-1).

Fig. 8:

- The non-personal data is stored with the following protection:

- Compliance validation and penetration testing;
- Encryption for Amazon RDS;
- Bit Keys;
- Database Logs;
- Backups.

Subscriber Data Access

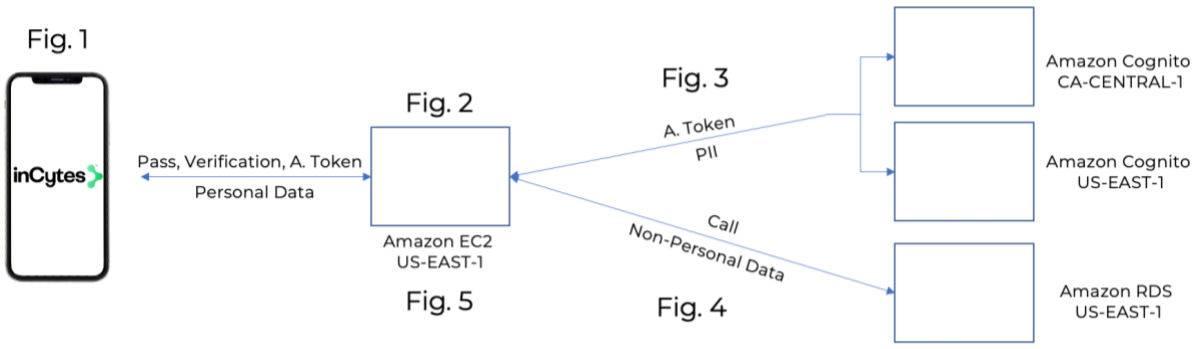

Fig. 1:

- Subscriber logs in, authenticating their identity through email, password and optional 2 factor authentication.

Fig. 2:

- Amazon EC2 Instance receives call for personal data and Authentication Token.

Fig. 3:

- Amazon EC2 routes Authentication Token to Amazon Cognito Servers;
- Upon validation, Amazon Cognito Servers return PII to the Amazon EC2.

Fig. 4:

- Amazon EC2 routes call for non-personal data to Amazon RDS;
- Amazon RDS returns non-personal data to Amazon EC2.

Fig. 5:

- Amazon EC2 replaces Subject ID with PII;
- Amazon EC2 returns personal data to device of authenticated User.

Key Considerations for Data Controllers using inCytes™

1. Select AWS Cognito Server Location;
2. Enable 2-Factor Authentication for Subscribers and/or their Patients;
3. Designate which fields in one's protocol might include PII;
4. Determine the Circle data sharing settings, including Personal Data or Non-Personal Data;
5. Upload Data Subject Consent Form;
6. If needed, craft Joint Controller Agreement.