

**TECHNICAL DESIGN DOCUMENT**

**Consent Management System**

**Version 1.0**

**May 18, 2020**

**Ipsen, Inc.**

**Prepared By**

|  |  |
| --- | --- |
| Document Owner(s) | Project/Organization Role |
| Axtria, Inc. | Vendor |

**Change Log**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Change Reference | Created by | Section |
| 18-May-2020 | 1.0 | Initial Version | Priya Bhatia |  |

Table of Contents

[1 DOCUMENT PREFACE 5](#_Toc40701430)

[**1.1** **Introduction** 5](#_Toc40701431)

[**1.2** **Purpose and Scope** 5](#_Toc40701432)

[**1.2.1** **Purpose** 5](#_Toc40701433)

[**1.2.2** **Scope** 5](#_Toc40701434)

[**1.3** **General Information and Version Details** 5](#_Toc40701435)

[**1.4** **Stakeholders** 6](#_Toc40701436)

[**1.5** **Abbreviations and Acronyms** 7](#_Toc40701437)

[2 DESIGN SPECIFICATIONS 9](#_Toc40701438)

[**2.1** **Problem Description** 9](#_Toc40701439)

[**2.2** **Key Technologies** 9](#_Toc40701440)

[**2.3** **System Overview** 10](#_Toc40701441)

[**2.4** **Resilience Measures** 11](#_Toc40701442)

[**2.5** **Backup Policy** 11](#_Toc40701443)

[**2.6** **Authentication and Authorization** 12](#_Toc40701444)

[3 TECHNICAL DESIGN 13](#_Toc40701445)

[**3.1** **Solution Architecture** 13](#_Toc40701446)

[**3.2** **System Integration** 14](#_Toc40701447)

[**3.2.1** **File-Based Integrations** 14](#_Toc40701448)

[**3.2.2** **One Trust Integration for CCPA Data** 15](#_Toc40701449)

[**3.2.3** **Profile Registrations on Ipsen Care or Brand Websites** 16](#_Toc40701450)

[**3.2.4** **Cross-Reference Process for HCPs** 17](#_Toc40701451)

[**Cross Referencing Process - HCPs** 17](#_Toc40701452)

[**3.2.5** **Match and Merge Process for Patients** 18](#_Toc40701453)

[**3.3** **Consent Processing** 20](#_Toc40701454)

[**3.3.1** **Processing of Dynamic Consent (HCP and Patients)** 20](#_Toc40701455)

[**3.3.2** **Consent Business Rules (HCPs)** 20](#_Toc40701456)

[**3.3.3** **Consent Business Rules (Patients)** 22](#_Toc40701457)

[**3.4** **PII Data Architecture (Illustrative)** 24](#_Toc40701458)

[**3.4.1** **File-Based Integrations** 24](#_Toc40701459)

[**3.4.2** **API-Based Integration** 25](#_Toc40701460)

[**3.4.3** **Encryption/Decryption Utility** 25](#_Toc40701461)

[4 SERVICE SPECIFICATIONS 26](#_Toc40701462)

[**4.1** **Data Sources** 26](#_Toc40701463)

[**4.1.1** **HCP and Patient Profile Sources** 26](#_Toc40701464)

[**4.1.2** **HCP and Patient Consent Sources** 27](#_Toc40701465)

[**4.2** **Third-Party Integration** 30](#_Toc40701466)

[**4.3** **User and Access Management** 30](#_Toc40701467)

[**4.4** **Servers** 32](#_Toc40701468)

[**4.4.1** **Application Servers** 32](#_Toc40701469)

[**4.4.2** **Database Servers** 32](#_Toc40701470)

[5 DATABASE SCHEMA SPECIFICATIONS 33](#_Toc40701471)

[**5.1** **Application-Level Schema** 33](#_Toc40701472)

[**5.2** **HCP-Level Schema** 38](#_Toc40701473)

[**5.3** **Patient-Level Schema** 48](#_Toc40701474)

# DOCUMENT PREFACE

## **Introduction**

This document provides a detailed view of technical and architectural documentation of the Consent Management System (CMS). It captures information on system overview, architecture, high-level and low-level design specifications, system integration, and data schema details of the CMS and its components.

## **Purpose and Scope**

## **Purpose**

This Technical Design Document (TDD) details the technical design for Consent Management System (CMS), which acts as central repository of all the consent related information, along with a query tool for generating screened target lists, compliance lists and viewing consent audit trail. The document intends to provide technical resources with an explanation of CMS’s design and architecture. It also provides recommendations to users on how to implement the available system functionalities for further development with an understanding of what has already been built, what is further to be built, and how it is expected to be built.

## **Scope**

This document contains technical documentation for all the modules for Consent Management System (CMS). CMS is a part of Ipsen’s effort towards managing the consent of its customers (both HCPs and patients), consistently and efficiently. This document focusses on the low-level design and crucial components while outlining its high-level architecture at the same time.

## **General Information and Version Details**

|  |  |
| --- | --- |
| Information | Detail/Description |
| Document Title | Consent Management System – Technical Design Document |
| Date of Release | 13-May-2020 |
| Product Version | 1.0 |
| Document Version | 0.1 |
| Document Owner | IPSEN Biopharmaceuticals Inc |
| Document Author | Axtria |

## **Stakeholders**

The section identifies Ipsen’s individuals/teams that have a vested interest/concern in the implementation of the Consent Management Application and those who are directly involved in using the application. Below is the panel of potential users who can actively participate in defining or making changes (if required) in the existing technical design and architecture:

|  |  |  |
| --- | --- | --- |
| Role | Unit | Name |
| IPSEN Business Users | Business Team |  |
| Marketing Users | Marketing Team |  |
| Technical Architect, Design Engineers, Integration team | Development Team |  |
| Project Managers | Project Management Team |  |
| Production representatives, Quality Control | Production Management |  |
| Support Services, Trainers | Support and Maintenance Division |  |
| Infrastructure representatives, managers | IT Infrastructure |  |

## **Abbreviations and Acronyms**

|  |  |  |
| --- | --- | --- |
| Abbreviation/Acronym | Expansion | Definition |
| CMA | Consent Management Application | A web-based, centralized data management tool that helps IPSEN to manage consent and queries of its customers (both HCPs and patients) consistently and efficiently. |
| HCP | Healthcare Providers | An individual/organization that provides a health care service to people |
| IPSEN | Innovation for Patient Care | A French pharmaceutical headquartered in France, indulged in developing and marketing medications used in oncology, neuroscience and rare diseases along with consumer healthcare products |
| API | Application Programming Interface | A computing interface which defines interactions between multiple software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow and so on. |
| DSAR | Data Subject Access Request | A written request made by or on behalf of an individual for the information which she is entitled to ask for under section 7 of the Data Protection Act 1998 (DPA) |
| SSO | Single Sign-On | An authentication scheme that enables users to securely authenticate with multiple applications and websites by logging in only once—with just one set of credentials (username and password). |
| IDP | Identity Provider | A trusted provider that lets you use single sign-on (SSO) to access other websites |
| SSL | Secure Socket Layer | A protocol developed by Netscape for transmitting private documents via the Internet. It protects transactions between your Web site and visitors |
| REST | Representation State Transfer | Defines a set of constraints used for creating Web services. Web services that conform to the REST architectural style, called RESTful Web services, provide interoperability between computer systems on the Internet. |
| PII | Personally Identifiable Information | Informational attributes used to identify a specific individual such as full name, mailing address, email address and the like. |
| HTTPS | Hypertext Transfer Protocol Secure | An extension of the Hypertext Transfer Protocol (HTTP), used for secure communication over a computer network. It is widely used on the Internet |
| NPI | National Provider Identifier | A unique 10-digit identification number issued to health care providers in the United States by the Centers for Medicare and Medicaid Services. |
| SFTP | Secure File Transfer Protocol | A secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. |
| CCPA | California Consumer Privacy Act | A state statute intended to enhance privacy rights and consumer protection for residents of California, United States |
| AMA | American Medical Association | American Medical Association |
| SMS | Short Message Service | Used for sending text messages to mobile phones |
| SFMC | Salesforce Marketing Cloud | A CRM platform for marketers that allows them to create and manage marketing relationships and campaigns with customers |
| CAN-SPAM | Controlling the Assault of Non-Solicited Pornography and Marketing Act | Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 |
| PDRP | Physician Data Restriction Program | Empowers physicians by allowing them to restrict pharmaceutical sales representatives from accessing their prescribing data |
| AWS | Amazon Web Services | A subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered pay-as-you-go basis |
| URL | Uniform Resource Locator | Specifies resources’ addresses on the World Wide Web |
| CPU | Central Processing Unit | A central processor or main processor, is the electronic circuitry within a computer in which operations are controlled and executed |

# DESIGN SPECIFICATIONS

|  |  |
| --- | --- |
| **Problem Description** |  |

IPSEN had growing concerns about having a well-designed permission marketing concept in place while keeping the necessary underlying influential aspects, i.e., *legal regulation, internal policy,*and*individual preferences into consideration*. These factors required the organization to have compliant processes established for processing customer data and conducting marketing communication. As part of their focussed efforts towards this problem has led to a solution that includes centralized data management of all customer consent for receiving communications and promotions. This system further provides an ability to query and screen customers for legal and regulatory purposes and to created targeted lists for campaigns. The key idea behind the solution is to have restricted access to users authorized by IPSEN who have a legitimate business purpose for accessing data and received pieces of training in IPSEN data privacy policies and principles before the initial access.

The overall context of consent management system, thus, illustrates the business process for:

* Profile registration and consent arriving into the Consent Management Application
* Opt-outs arriving through various channels like Axtria Email, integrated CRM network (Veeva) and third-party vendors etc.

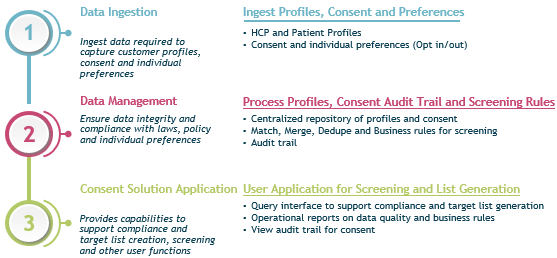
## **Key Technologies**

The following table lists down the technologies used by Consent Management Application.

|  |  |
| --- | --- |
| Technology | Version |
| Python | Version 3.6 |
| Django | Version 2.1.11 |
| AWS RDS | Postgres 10.7 |
| AWS S3 |  |
| AWS Glue | Version 1.0 |
| Elastic Beanstalk | Version 2.9.10 |

## **System Overview**

IPSEN Biopharmaceuticals Inc. partnered with Axtria to streamline the management of their customers’ consent and profiles by creating a Consent Management System. This system enables IPSEN to manage and query the consent of its customers, both patients and healthcare providers, more consistently and efficiently.

The core system function includes a centralized data management platform for handling customers’ consent, profiles, and individual preferences for receiving communications and promotions, along with the modules to query and screen customers for legal and regulatory purposes, and to create target lists for campaigns. Additionally, the guiding principle for accessing this solution is to have restricted access to only those data elements, which are necessary to perform legitimate business purposes by authorized individuals.

Let’s have a brief understanding of the project system overview. The figure on the right, depicts the entire concept of this system, which provides the information to have a good sense of the capacity of the system, its components, what the system does, what actions each system component performs, and what they can interact with.

**Data Ingestion**

Data ingestion component ingests data required to capture customer profile (HCP and patient profiles), consent, and individual preferences of customers (opt-ins/opt-outs).

**Data Management**

This component's primary function is to ensure data integrity and compliance with laws, policy, and individual preferences. It offers a centralized repository of all customer consent and profiles for receiving communications and promotions, match, merges, and dedupe business rules for screening. The component also helps to maintain an audit trail to capture consent changes to enable transparency into the current state of consent and all changes made over time.

**Consent Application**

At a high-level, the application provides a query interface with capabilities to support compliance and target list creation, screening, and other useful functions such as viewing operation reports on data quality and business rules and audit trail for consent.

## **Resilience Measures**

Ipsen’s Consent Management system operates in a Serverless / Platform as a service environment. The Serverless / Platform as a service architecture creates an execution model wherein the cloud provider runs the server and dynamically manages the allocation of machine resources. It then auto-assigns theses resources, thereby maintaining the overall load across multiple resources access.

The Application is designed to handle a maximum of ten users concurrently while being flexible enough to add more users in future. The architecture is built by using AWS cloud services (database, as well as web application). Hence it would be feasible to scale it in future (horizontally or vertically) as the usage pattern increases.

## **Backup Policy**

The system backup runs once a day, and the system retains the backup data for the last 35 days.

* 1. **Authentication and Authorization**

**Authentication**

All individuals having access granted to Consent Management Application (query tool/front-end), receive rigorous data privacy and security training before allowing complete access to the solution. The specific criteria (such as training and roles) required to get fulfilled before granting the access are solely at the discretion of IPSEN and is defined and approved by the team only. Any pieces of training or other criteria deemed necessary to get approved for the authentication will be monitored outside the consent management system.

Authentication requisites include controlled access to the app requiring a username and a password, with the logout action enabled.

**Authorization**

Authorization controls what actions each user can perform once she successfully logs into the Consent Management Application. IPSEN must recommend and approve a specific authorization group to a user/individual before enabling the functional access in the system. Any pieces of training or other criteria deemed necessary to get approved for the authorization group will be monitored outside the consent management system.

IPSEN to enable the following authorization groups within the consent solution and assign an individual a group with the capabilities, as listed below:

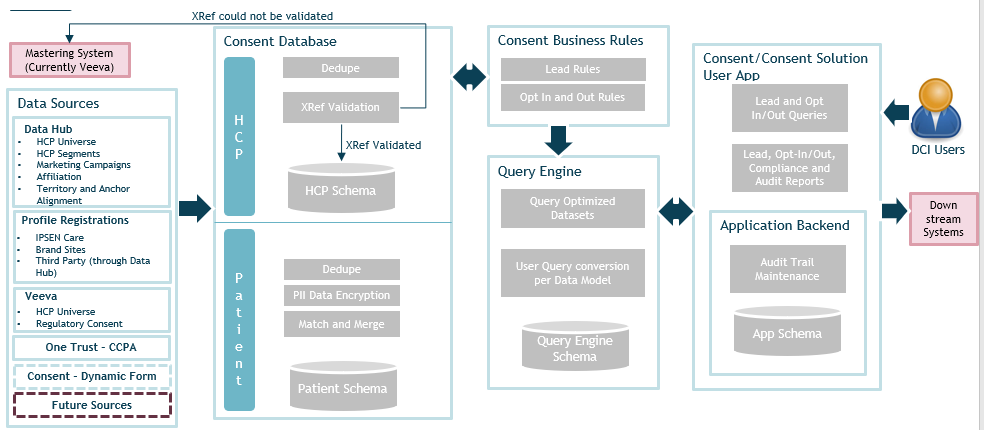
|  |  |
| --- | --- |
| Group | Key Functions Enabled |
| Analysts | * Query and view data related to HCPs, Patients or both HCPs and Patients depending on approved authorization * Save queries for reuse and share questions with other users of the consent solution * Access and reuse query saved by them or shared with them. * Export target lists to box |
| Analysts with Unmasked Access | * All functions enabled for the Analyst group, plus the access to unmasked data on the list preview screens for patients |
| IPSEN Business Team | * All functions enabled for the Analyst group, plus * Access, view, edit, and delete all queries created within the system. * Access to unmasked data on the list preview screens for patients * View existing or current business rules configured in the system. * Review all business rule changes requested by other users and, as appropriate, request changes from the Consent Admin |
| Administrators | * Admin role assigned to one or more individuals in the vendor team supporting the consent management solution * Manage all user onboarding and offboarding, data and rule related service requests and ad hoc requests |

# TECHNICAL DESIGN

## **Solution Architecture**

The Consent Management Solution integrates with specific pre-approved data source networks to enable the requirements contained within the system.

These data sources primarily include Data Hub, Profile Registrations, Veeva network and Consent sources. The data hub captures source elements such as marketing campaigns, HCP segments, affiliation, and territory alignment. Profile registrations source from IPSEN care and brand websites, third-party channels. For more information on data sources, please refer to [section 4.1](#_4.1_Data_Sources). The solution database captures the consumer details from these sources, dedupes the information, and stores the data into the database schemas after performing all the necessary validations. The data is then fetched for further processing by the query engine after the system incorporates and applies the business rules determined and approved by Ipsen.



***Figure 1: Solution Architecture – Consent Management Application***

At this point, the following data source integrations are not available:

* Ipsen Care: unavailability of data from upstream
* Brand Sites: unavailability of data from upstream
* Consent – Dynamic Form: Dynamic forms are not in place. The integration will be done when the forms are in place.

Once the data is processed, the system makes the processed data available to Consent Management user application. The app provides a query interface with capabilities to support compliance, auditing, target list creation, screening, and other useful functions such as viewing operation reports on data quality and business rules and audit trail for consent.

Additionally, the application offers the capability to push the data to downstream systems (currently box. SFMC and other connectors can be added future).

## **System Integration**

To enable the requirements contained within, the Consent Management System integrates with various data source networks (the details of data sources is defined in section 4.1).

All the integrations except for below are file-based:

1. One Trust integration for CCPA data – this is API based integration
2. File export to Box – this is API based integration

The Consent Solution incorporates and applies consent related business rules determined and approved by Ipsen. These rules enable consent application in a consistent and agreed way. Using these rules will help Ipsen marketing teams comply with approved marketing, legal and regulatory requirements. The overall system design accounts for the consumption of customer profiles, consent related opt-ins/out on currently used channels, while also enabling new avenues to be added quickly.

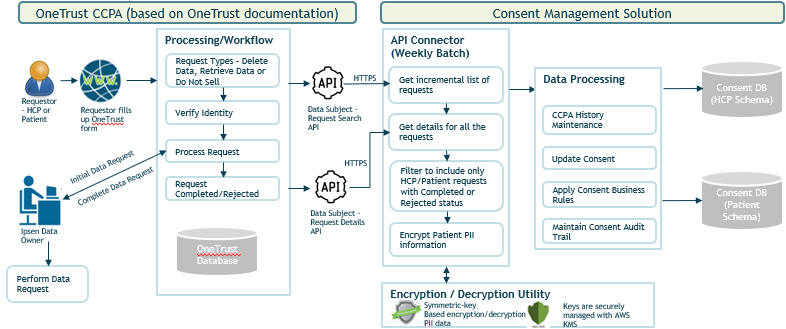
## **File-Based Integrations**

Data Hub, Veeva and profile registration data from Ipsen care and brand websites, are all file-based integrations.

1. Sources push the data to FTP site or S3.
   1. Veeva pushes the data to FTP site.
   2. Data Hub pushes the data to workbench S3 bucket.
   3. Ipsen care and Brand websites are assumed to push data in S3 bucket.
2. Automated glue jobs read the data from file and push to staging schema of the database.
3. Automated glue jobs read the data from staging schema, convert to required data model and push to HCP/Patient schemas.

## **One Trust Integration for CCPA Data**

Below figure depicts the sequence of events that occur to integrate CCPA data to the Consent Management system:



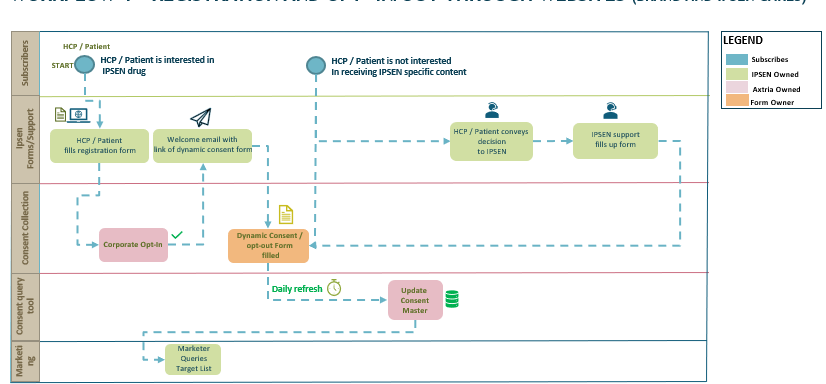
***Figure 2: Integration Architecture – Consent Management Application***

Ipsen’s Consent Management Solution interacts with OneTrust, privacy, security, and trust platform via a dynamic web form aimed to capture a consumer’s (HCP/Patient) request. This communication, in turn, initiates a workflow to process that request. OneTrust interacts with both consumers and system owners via emailers at several different checkpoints. Consumers will use their web browsers, either desktop or mobile, to upload files to confirm their identity. Systems owners access the DSAR Admin UI via SSO utilizing Ipsen’s IDP to view and process requests assigned to them.

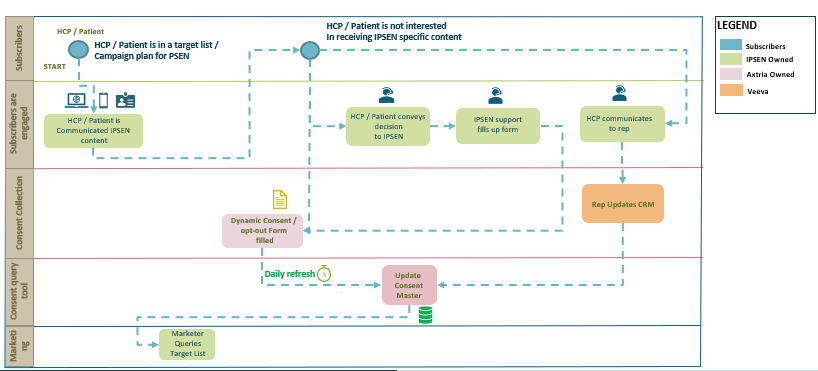
Once requests have been rejected or completed, their details can be extracted through a REST API provided by OneTrust. The API is protected by a key which is generated for each downstream system. OneTrust also supports the ability to restrict incoming API communications to a specific IP address. All communications with the REST API are secured through SSL. OneTrust further relays this information to the Consent Management Solution via API connectors (weekly batch) wherein it gets incremental lists of all requests along with their details. It further filters the data to include only HCP’s and patients’ requests with rejected and completed statuses, then encrypt patient PII information with the help of encryption/decryption utility system. After this, the system processes data further and stores it into the consent database schema.

## **Profile Registrations on Ipsen Care or Brand Websites**

The context of Ipsen’s consent management system, thus, illustrates the business process flow for profile registration and consent (opt-ins) arriving into the Consent Management Application. It also demonstrates the business process flow for op-outs coming from the dynamic form and the integrated Veeva network.

******The process flow diagrams below depict a series of actions that provide a broad overview of these processes to define how they are carried out, allowing for easier analysis and process improvement:

***Figure 3: Business process flow for Profile Registration and Consent arriving into CMA***



***Figure 4: Business process flow for an opt-out arriving through the dynamic form and Veeva***

## **Cross-Reference Process for HCPs**

Consent Management System (CMS) cross references the consent, profile and marketing engagement related information coming from various sources, with the universe of HCP/Patient. The purpose is to link all the transactional data with the universe (reference data).

The process flow diagrams below depict a series of actions that provide a broad overview of these processes to define how they are carried out, allowing for more accessible analysis and process improvement.

## **Cross Referencing Process - HCPs**

The profile, opt-out or marketing engagement related data ingested by the system subjects to the following cross-referencing steps and data validation rules:

**Step 1:** System maintains an Axtria ID against all records

**Step 2:** If the incoming profile does not have either an NPI ID or a combination of the First Name, Last Name, and Email Address. If even one is unavailable, the system will maintain it as a bad record.

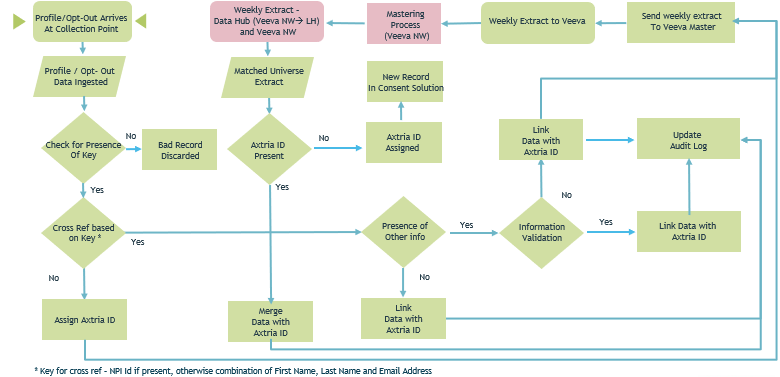
**Step 3:**If the system validates the previous step and all the three fields are available, the system performs a lookup on the key – The key can either be the NPI ID(Primary Key) if present or a combination of the First Name, Last Name and the Email ID (Secondary Key) if NPI is unavailable

**Step 4:**If the incoming data has a match, the system checks for other attributes:

1. If other attributes are not present, the system links the data to a unique Axtria assigned identifier and updates the audit log.
2. If other attributes are present, the system validates these records, links it to a unique Axtria assigned an identifier, and updates the audit log. Other attributes = Address, Phone Number
3. If other attributes are present but do not match, the system updates audit log against the linked Axtria ID; the system still throws the records toward the mastering process

**Step 5:**The system ingests a weekly feed from Veeva

1. If the incoming data does not have an Axtria ID assigned to it, the system treats it as a new record
2. If the incoming data has an Axtria ID assigned to it, a merge action is performed, and the audit log is updated.

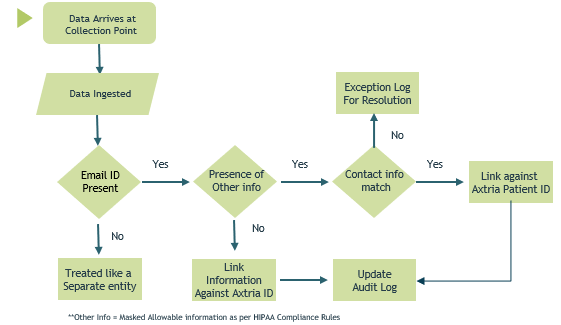
******

***Figure 5: Patient Information Validation and Cross-Referencing Rules***

## **Match and Merge Process for Patients**

The system uses the following keys to determine if the incoming profile has an:

* Email ID- Used as the primary key
* Secondary Key – First Name and Last Name





***Figure 6: HCP Cross Referencing Rules – Consent Management Application***

The system screens a profile as per the following steps:

**Step 1:** If the incoming batch of profiles has multiple records with the same email ID, the system treats the latest one for consideration for the match-merge process

**Step 2:** If the incoming profile does not have an email ID, the cross-referencing process is not successful, it is treated as an invalid record and added to the exception log. These records are labeled invalid.

**Step 3:** If the incoming profile has First Name, Last Name, and an email ID but does not match in the system, it will treat it as an additional entry to the universe that the system maintains

If the incoming profile data is matched based on email ID:

1. The system links the information with the universe and allows the user to query this information
2. A secondary check occurs for the presence of other data. Other data for patients includes First Name and Last Name in the current version of the application
3. f First Name and Last Name are available in the system; the system performs a matching process against these in the order. When the match-merge process completes, the system updates the rest of the information (like physical address and phone number) based on the latest record that has arrived. The universe entry is thus updated with the same information
4. If the Match Process is unsuccessful in the First Name and the last name, the system allows querying on the information that was placed historically in the system. The system also maintains these records in the exception log.

If other data is present, the system checks for additional data fields such as location attributes. These do not match. In case the method throws an exception, it will maintain the data in a separate exception log:

The system currently classifies the incoming records into five different categories:

* Invalid Record – Wherein, any of the First Name, Last Name, and Email Address, is not found in an incoming profile
* Universe Mastered Record – A profile collected by the system previously
* Duplicate records – These are duplicates in the current batch. The latest record is picked for further classification, from the set of copies.
* Matched Record - The current record matches the existing entry in the universe, based on primary and secondary matches. The rest of the information (like physical address, phone) is fetched from the latest record, and universe entry is updated for the same.

Unmastered Records – In case both all the keys expected by the system, i.e., Email ID, First Name, and Last Name, are present in the system.

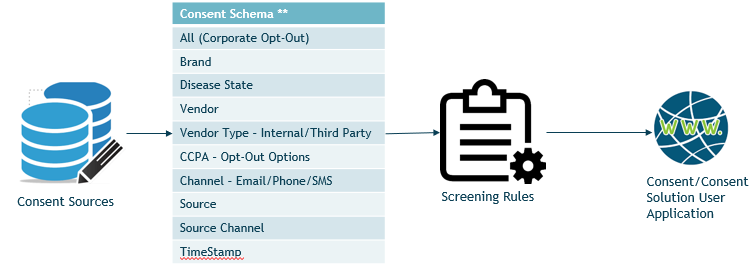
## **Consent Processing**

The consent processing mechanism of Ipsen’s Consent Management Solution runs on some pre-defined business rules for both HCPs and patients. Before discussing these rules in-depth, let’s understand the system processing of dynamic requests of all customers.

## **Processing of Dynamic Consent (HCP and Patients)**

The system is capable of processing ongoing consent at the most minute levels of granularity. It stores all the dynamic consent as indicated with the standards of the hierarchy of a US Corporate Opt-Out, Band, Disease State, Vendor, Vendor Type-Internal / Third Party, flags related to CCPA, Channel (communication mechanism for which the user has opted out), source of the arrival of the opt-in/opt-out, and the stored time of entry.

The general guidance form Ipsen legal is that HCPs and patients who opt-out to Ipsen promotions or communications automatically opts-out at the corporate level (all channels) if they are not provided with more granular choices (i.e., at the brand, therapeutic area or channel). In the current state (as of May-2020), the dynamic forms are not in place. Hence all the opt outs (except third party) are corporate opt outs.

*****Figure 7: Consent Processing and Business Rules***

## **Consent Business Rules (HCPs)**

**Initial Consent Rules**

The below rules apply for initial consent, which means that consent rules are set while initializing the Consent Management system:

**Opt-In Business Rules**

* The system considers all Veeva Network Mastered HCPs as a US Corporate Opt-in for all channels in scope except for SMS and Fax, unless opted out
* SMS and Fax require an explicit opt in

**Opt-Out Business Rules**

**Business Rules (based on Regulatory Opt-Out)**

* If the AMA **Do Not Contact** flag is enabled, HCP is US Corporate Opt-Out
* PDRP Flag is just to enable querying for information. System does not perform any action to screen HCP
* CCPA Data Delete Request (if received from the OneTrust solution): The system screens out this profile on all available channels while retaining the related consent information

**Business Rules (based on Preference Opt-Out)**

* Veeva Network: If any preferential opt-out flag from Veeva Network is true, HCP is US Corporate Opt-out
* Veeva Approved Rep Emails: If an HCP has unsubscribed to a rep approved email historically, HCP is US Corporate Opt-out
* IPSEN Cares Website (if opt outs are available): HCP is a US Corporate Opt-Out.
* Brand Websites (if opt outs are available): HCP is a US Corporate Opt-Out.
* Salesforce Marketing Cloud opt outs: HCP is a US Corporate Opt-Out

If Opt-out date is available, the system considers opt-out from 2019 and onward

**Ongoing Consent Rules – Prior to the Availability of the Dynamic Consent Forms**

**Opt-In Business Rules**

The business rules for opt-in continue to be applicable until the launch of the dynamic forms.

**Opt-Out Business Rules:**

Regulatory Opt-Outs: The rules for the Regulatory Opt-Outs from section 3.2.1 continues to be applicable until the launch of dynamic forms.

**Business Rules (based on Preference Opt-Outs):**

* The rules from section 3.2.1 continues to be applicable in the case of Veeva Network, Veeva Approved Rep Emails, IPSEN Cares Websites (if opt-outs are unavailable), Brand websites (if opt-outs are available) and SFMC opt-outs until the launch of the dynamic forms.
* Opt-Out from a third-party channel, if shared, results in the HCP being opted out of all communication from on that third-party channel only

**Ongoing Consent Rules - Post Availability of the Dynamic Consent Form**

**Opt-In Business Rules**

Opt-Ins: The business rules for opt-in from Section 3.2.1 continues to be applicable until the launch of the dynamic forms.

**Opt-Out Business Rules:**

**Business Rules (based on Regulatory Opt-Outs):**

* If the AMA Do Not Contact flag is true, HCP is US Corporate Opt-Out
* CAN-SPAM: Opt-outs to be honoured in 10 days
* CCPA Data Delete Request: The system screens out this profile on all available channels while retaining the related consent information

**Business Rules (based on Preference Opt-Outs):**

* If preferential opt-out flag from Veeva Network is true, HCP is US Corporate Opt-Out
* If an HCP uses the Dynamic Consent Forms to opt out from a therapeutic area, brand, channel or a 3rd party
  + Opt-Out from a channel opts HCP out from all IPSEN communications from that channel for all brands
  + Opt-Out from a brand or therapeutic area opts HCP out of all IPSEN communications for that brand / therapeutic area
  + Opt-Out by selecting “Corporate” on the dynamic form will result in the HCP being opted out of all IPSEN communications
* Opt-Out from a third-party channel, if shared, results in the HCP being opted out of all communication from on that third-party channel only

## **Consent Business Rules (Patients)**

**Initial Consent Rules**

**Opt-In Business Rules**

* All Patients who opted-in historically are US Corporate Opt-Ins, unless specifically opted out
* All third-party profiles are set as a corporate opt in if system agrees upon the appropriate consent

**Opt-Out Business Rules**

**Business Rules (based on Preference Opt-Out)**

* SFMC Email Opt-Outs (from 2019): If any preferential opt-out flag from SFMC Unsubscribe Forms, Patient is US Corporate Opt-Out
* IPSEN Cares Brand Websites (if available, from 2019): If any preferential opt-outs are available from IPSEN Cares, the system considers the patient as a US Corporate Opt-Out
* Brand Websites (if available, from 2019): If any preferential opt-out flags are present from Brand Websites, the system considers the patient as a US Corporate Opt-Out.

If Opt-out date is available, the system considers opt-out from 2019 and onward

**Ongoing Consent Rules – Prior to the Availability of the Dynamic Consent Forms**

**Opt-In Business Rules**

* All Patients who opted-in historically are US Corporate Opt-Ins, unless specifically opted out
* Specific opt-ins required for SMS and Fax

**Opt-Out Business Rules:**

**Business Rules (based on Preference Opt-Outs):**

* SFMC Email Opt-Outs: If any preferential opt-out flag from SFMC unsubscribe Forms of ongoing campaigns, Patient is US Corporate Opt-Out
* IPSEN Cares Brand Websites (if available): If any preferential opt-outs are available from IPSEN Cares, Patient is US Corporate Opt-Out
* Brand Websites (if available): If any preferential opt-out flags are present from Brand Websites, patient is a US Corporate Opt-Out.

**Ongoing Consent Rules - Post Availability of the Dynamic Consent Form**

**Opt-In Business Rules**

* All Patients who opted-in historically are US Corporate Opt-Ins, unless specifically opted out
* Specific opt-ins required for SMS

**Opt-Out Business Rules:**

**Business Rules (based on Regulatory Opt-Outs):**

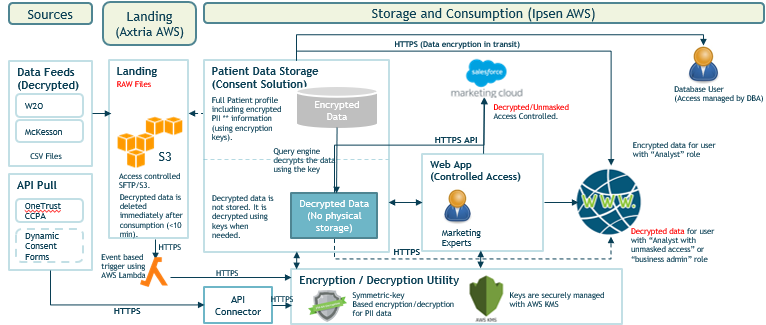
* CAN-SPAM: Opt-outs to be honoured in 10 days
* CCPA Data Delete Request: The system screens out this profile from all possible target lists while retaining the consent information

**Business Rules (based on Preference Screening):**

* If a patient uses the dynamic consent form to opt out from the corporate, therapeutic area, brand, channel or a 3rd party
  + Opt-out the corporate level opts the patient out of all communications
  + Opt-out from a channel opts patient out from all IPSEN communication from that channel, across all brands
  + Opt-out from a brand or therapeutic area opts Patient out of all IPSEN communication for that brand /therapeutic area
  + Opt-out from a third party (if shared by third party) opts patient out of all communication via that third party

## **PII Data Architecture (Illustrative)**

The below architecture depicts, how the consent management system handles the processing and storage of Patient PII information. Note that PHI information is not needed for any of the consent use cases, hence the system does not process/store any PHI related information.

***Figure 8: PII Data Architecture – Consent Management Application***

Below is the list of PII fields expected to flow in the system:

1. First Name
2. Last Name
3. Email
4. Phone
5. Street Address
6. Zip Code

## **File-Based Integrations**

W2O and McKesson, vendors for brand website and IPSEN care respectively, support sharing of information, in form of flat files only. Consent system follows the below approach to make sure of data security. With this, it is made sure, decrypted information does not stay anywhere in the storage, for more than 10 minutes.

1. Vendors push the data in decrypted and identifiable format to Axtria managed S3 bucket.
2. Using, S3 event-based triggers, a lambda function is triggered to consume the file almost immediately.
   1. Encrypt all the PII related data using encryption/decryption utility
   2. Move the data to consent storage.
   3. Delete the decrypted copy of data from S3 bucket.

## **API-Based Integration**

One Trust CCPA system in current state has the API endpoints available, for consent system to pull the data directly, without the need of a landing layer in between. Dynamic form system is not currently in place. But same is also assumed to support similar type of integrations, to ensure tighter security.

Consent system follows the below approach to make sure of data security.

1. Secure API connector (part of consent system) connects to the upstream API endpoint (SSL/TLS endpoint).
2. The connector encrypts the PII data (using encryption/decryption utility), within transit itself.
3. The connector moves the encrypted data to consent storage.

## **Encryption/Decryption Utility**

The PII architecture relies on an encryption/decryption utility to secure the personal data of all patients. The configuration includes the encryption of PII data encryption, and key management.

The utility manages the encryption keys via the AWS Key Management Service (KMS). It implements the symmetric key algorithm, which uses the same cryptographic keys for both encryptions of the plain text and decryption of the ciphertext. The keys are not stored in consent system anywhere. It just connects to the KMS through IAM roles.

**About AWS KMS:**

AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

# SERVICE SPECIFICATIONS

## **Data Sources**

The data sources of Ipsen’s Consent Management Solution primarily include HCP profile sources, patient profile sources, HCP sources of consent, and patient sources of consent. Let’s discuss these sources in detail.

## **HCP and Patient Profile Sources**

HCP and Patient profiles from the following sources initialize the Consent Management Solution

|  |  |
| --- | --- |
| HCP Profile Sources | Patient Profile Sources |
| * Registrations on Brand Websites | * Registrations on Brand Websites |
| * Registrations on IPSEN Cares Websites or those that come in by fax. | * Registrations on IPSEN Cares Websites or those that come in by fax. |
| * Uninvited HCPs who attend events (virtual events, speaker programs and trainings) | * Patient Registrations on 3rd Party Websites |
| * Registrations for Dysport Injector trainings at the CLIMB website | * Patient Registration on Point of Care Applications |
| * Profiles received from 3rd party sources such as Medscape |
| * Profiles received from 3rd party peer to peer engagement sources such as Peer Direct |

The Consent Management Solution ingests the profile data from these sources and set the consent information based on approved business rules. Sources can be added incrementally if required. The system design is flexible to incorporate additions of sources.

## **HCP and Patient Consent Sources**

The Consent Management system sets the initial consent (whether an HCP/patient has opted-in or out) based on the available information and Ipsen “initial consent business rules”.

As the system captures the consent changes, it will process them based on the “ongoing or dynamic consent business rules” enabled.

|  |  |  |
| --- | --- | --- |
| Source Type | HCP Consent Sources | Patient Consent Sources |
| Initial Consent Sources | **Opt-in Sources:**  Veeva Network | **Opt-in Sources:**  Brand Websites, IPSEN Cares, 3rd Party Websites – Healthy Offers, 3rd Party Point of Care Applications – E.g. Phreesia |
| **Regulatory Opt-Out Source:** Veeva  **AMA Do Not Contact Flags**🡪 *sourced by Veeva Network from Veeva Open Data and represents the regulatory optout from the AMA Masterfile*  **AMA** **PDRP** **Flags🡪** sourced by Veeva Network from Veeva Open Data and represents the regulatory restriction of share of prescription data with reps. Veeva system captures the opt-out date and enable the field for querying | **Preference Opt-Out Business Sources**   * Unsubscribed Patients from IPSEN SFMC Email Campaigns (2019) * IPSEN Cares (if available) * Brand Websites(if available) * CCPA Data Delete Requests: One Trust Integration (if available) |
| **Preference Opt-out Sources:** Veeva  **Data** **Privacy** **Opt**-**Out** **Flag**🡪 *sourced from Veeva Open Data and represents a data share opt-out captured from Veeva Network*  **HCP** **Opted** **out** **in** **IPSEN** **Flag**🡪Custom Opt-Out Flag maintained at Veeva CRM and represents a Data Share Opt-Out captured from Veeva  **Veeva Approved Email Opt-Out Flag** (from Veeva CRM) – Email Opted out from by HCP or updated by rep  **Additional Opt-Out Flag🡪** Custom Opt Out Flags maintained for IPSEN  **Unsubscribed HCPs from IPSEN SFMC Email Campaigns sourced from Marketing Data Hub**  **CCPA Data Delete Requests:** One Trust Integration |
| Ongoing Consent Sources (Before the Availability of Dynamic Consent Forms) | **Opt-In Sources:**   * Veeva Network Mastered HCPs * New HCP registrations at Brand Websites (Dysport CLIMB, Somatuline Depot Net, Somatuline Acromegaly, Onivyde), IPSEN Cares (all brands), and any other source incrementally added | **Opt-In Sources:**  Brand Websites (Somatuline Depot Net, Somatuline Acromegaly, Increlex) and IPSEN Cares (all brands) |
| **Regulatory Opt-Out Sources**  Source of CCPA Requests from OneTrust and the following requests recorded in the Consent Solution database. Only the data delete request results in an opt out (at the corporate level):   * No-Sale Requests * Data Delete Requests * Information Requests for captured data * The source of HCP Regulatory Flags (other than CCPA) in Veeva Network * AMA Do Not Contact * PDRP | **Preference Opt-Out Sources:**   * Unsubscribed Patients from IPSEN SFMC Email Campaigns * IPSEN Cares (if data available) * Brand Websites (if data available) * CCPA Data Delete Requests: One Trust Integration |
| **Preference Opt-Out Sources:** Veeva   * Data Privacy Opt-Out Flag * HCP Opted out in IPSEN Flag🡪Custom Opt-Out Flag maintained at Veeva CRM. * Additional Opt-Out Flag 🡪 Custom Opt Out Flags maintained for IPSEN * Veeva CRM (via the Marketing Data Hub) * Email Unsubscribes from the Veeva Approved Emails * Unsubscribed HCPs from IPSEN SFMC Email Campaigns sourced from Marketing Data Hub * IPSEN Cares (if data available) * Brand Websites (if data available) * **CCPA Data Delete Requests**: One Trust Integration |
| Ongoing Consent Sources (Post Availability of Dynamic Consent Forms) | **Opt-In Sources:**   * Veeva Network Mastered HCPs * Dynamic Consent Form changes * New HCP registrations at Brand Websites, IPSEN Cares, Speaker Programs and Events, any other source incrementally added | **Opt-In Sources:**   * Brand Websites * IPSEN Cares * Third Party websites (if any) * Any other sources incrementally added |
| **Regulatory Opt-Out Sources:**   * Source of CCPA Requests: One Trust Application * No-Sale Requests * Data Delete Requests * Information Requests for captured data * Source of HCP Regulatory Flags (other than CCPA) is Veeva Network * AMA Do Not Contact * PDRP | **Regulatory Opt-Out Sources:**   * Source of CCPA Requests: One Trust Application * No-Sale Requests * Data Delete Requests * Information Requests for captured data |
| **Preference Opt-Out Sources:**   * Data Privacy Opt-Out Flag * HCP Opted out in IPSEN Flag🡪Custom Opt-Out Flag maintained at Veeva CRM. * Additional Opt-Out Flag 🡪 Custom Opt Out Flags maintained for IPSEN * Veeva CRM (via the Marketing Data Hub) * Email Unsubscribes from the Rep-Approved Email Data or from Dynamic Consent Forms * IPSEN Cares via the Dynamic Consent Forms * Brand Websites via the Dynamic Consent Forms * CCPA Data Delete Requests: One Trust Integration | **Preference Opt-Out Sources:**  Dynamic Consent Form for IPSEN-owned channels |

## **Third-Party Integration**

The Consent Management Solution uses the following third-party vendor integration for communicating and promoting to HCPs:

|  |  |  |  |
| --- | --- | --- | --- |
| Communication Channel | Information Source | Third Party/In house/Agency | Point of Contact |
| Email | Axtria | Agency | Axtria |
|  | Biopharm | Third Party | Jaclene C. D'Ambra (BioPharm Communications) <jdambra@biopharmcommunications.com> |
| Peer to Peer | Peer Direct | Third Party | Tara Kuboski <tara.kuboski@peerdirect.com> |
| Web | WebMD (multiple tactics – display, email) | Third Party | Communication with: dnathanson@webmd.net |
| Medscape ((multiple tactics – display, email)) | Third Party |
| PHM | Third Party | NA (Display Ads not assumed to be person-specific in nature) |
| Events | Phoenix (eNova) | In House | Communication sent to: Marc Bunn <[mbunn@teamenova.com](mailto:mbunn@teamenova.com)>  Communication received from: Tracy Spencer <[tspencer@teamenova.com](mailto:tspencer@teamenova.com)> |
|  | Medical Leverage | In house | Communication sent to Kirstin Croucher <[kcroucher@medicalleverage.com](mailto:kcroucher@medicalleverage.com)>  Communication received from Maureen Legaria <mlegaria@medicalleverage.com> |
| Social | Epocrates | Third Party | Communication Sent To: Kate Eucker  Communication Received from: Brian Parker <brparker@athenahealth.com> |
|  | Doximity | Third Party | Ethan Hort <[ehort@doximity.com](mailto:ehort@doximity.com)> |

## **User and Access Management**

The Consent Management system enables an access management framework for different user roles, which provides them the ability to use a specific service or a group of functions. This framework includes the execution of policies and actions defined in information security management. The diagram below depicts the entire process workflow for PII data access and protection, which enables you to understand the concept of access management in CMA:

The system has all the user roles defined in requirements stated in the authentication. It controls and monitors the users who can access the front-end of the application. As you see in the figure that the system enables the PII information across all the patient data sources in a controlled and encrypted format. The users (marketing experts) extract the info to access controlled buckets on the box folders to provide access to the following sets of users:

* IPSEN internal users
* Third-party users who might run campaigns on behalf of IPSEN
* The database administrator in-charge of keeping control of the numbers of users having access to the system. She maintains credentials for backend users during the operation phase and maintains logs for the same.

The consent management system maintains the detailed audit logs for system access and supports the functions/solutions listed below:

* All sources send data to the consent system through S3/SFTP folders configured in the system.
* The system stores all encryption keys in a protected cloud environment.
* The maintenance and support users from the backend can access this encrypted data. However, without the encryption key, they or other app users cannot decode the data.
* The system deposits files in a clear text format to the server for the following purposes.
  + Marketing campaigns run by IPSEN or third-party users
  + Compliance-specific actions performed by IPSEN or third-party users.
* The system undergoes mechanisms to decrypt the data in transit and deposit a clear-text CSV file to the box folder.
* The system allows controlled access to this box folder for usage with the downstream systems.

## **Servers**

## **Application Servers**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Development | Test | Live |
| AWS Account Id | 6787-5412-5809 | 6787-5412-5809 | 7758-2994-5410 |
| Service Type and Name | Elastic Beanstalk (PaaS) application: consent-webapp | Elastic Beanstalk (PaaS) application: consent-webapp | Elastic Beanstalk (PaaS) application: consent-webapp |
| Environment Name | ConsentWebapp-env | ConsentWebapp-env-qc | ConsentWebapp-env-prod |
| URL | <http://consentwebapp-env.eba-yusbvm4n.us-east-1.elasticbeanstalk.com/> | <http://consentwebapp-env-qc.us-east-1.elasticbeanstalk.com/> | [https://consent.Ipsen.com](https://consent.ipsen.com) |
| CPU Cores | 2 vCPU | 2 vCPU | 2 vCPU |
| Memory | 7.5 GiB | 7.5 GiB | 7.5 GiB |
| Operating System | Amazon Linux 2.9.6 | Amazon Linux 2.9.6 | Amazon Linux 2.9.6 |
| Software and versions | Python 3.6, Django, Apache HTTPD | Python 3.6, Django, Apache HTTPD | Python 3.6, Django, Apache HTTPD |

## **Database Servers**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Development | Test | Live |
| AWS Account Id | 6787-5412-5809 | 6787-5412-5809 | 7758-2994-5410 |
| Service Type and Name | Aurora Postgres Serverless | Aurora Postgres Serverless | Aurora Postgres Serverless |
| Cluster Name | Consent-management-project-postgresrds | Consent-management-qc | Consent-management-postgres |
| Configuration | 2 to 16 Unites (auto scaling) | 2 to 16 Unites (auto scaling) | 2 to 16 Unites (auto scaling) |
| Software and versions | Postgre SQL 10 | Postgre SQL 10 | Postgre SQL 10 |
| Dependencies | NA | NA | NA |

# DATABASE SCHEMA SPECIFICATIONS

Consent Management Solution’s data schema covers the data models at application-level, HCP-level, and patient-level. Each of these data models is discussed in subsequent sections:

## **Application-Level Schema**

###### Auth\_User (User Authentication)

The table provides authorization details of users.

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| id | INTEGER | Authenticated user ID |
| password | VARCHAR | Authenticated user password |
| last\_login | TIMESTAMP | Indicates the time (with the time zone details) when the user last logged into the application |
| is\_superuser | BOOLEAN | Indicates whether the logged in user is a super admin |
| username | VARCHAR | Authenticated username |
| first\_name | VARCHAR | Identifies user’s first name |
| last\_name | VARCHAR | Identifies user’s last name |
| email | VARCHAR | Identifies user’s email address |
| is\_staff | BOOLEAN | Indicates whether the logged in user is a staff user |
| is\_active | BOOLEAN | Indicates whether the logged in user is an active user |
| date\_joined | TIMESTAMP | Indicates the date (with the time zone details) when the user onboarded the application |
| user\_id | INTEGER | Authenticated user ID |
| permission\_id | INTEGER | User’s permission ID |

###### permissions (access permissions)

This table details regarding the permissions available to users.

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| permission\_id | INTEGER | Unique identifier assigned to the permissions for the |
| permission | VARCHAR | The type of permission to be assigned |

###### ROLES (USER ROLES)

This table details regarding the roles available to users.

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| ROLE ID | INTEGER | Unique identifier of the record |
| ROLE | VARCHAR | Unique identifier of the user who was assigned the role |

###### dataset\_ref (dATASET REFERENCE)

Dataset ref details out the basic query datasets available to users.

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| connection\_ref\_id | INTEGER | Reference ID of the connection being used |
| dataset\_group | VARCHAR | If the dataset belongs to an HCP or a patient |
| dataset\_name | VARCHAR | Name identifier of the dataset. E.g.: HCP Universe |
| dataset\_disp\_name | VARCHAR | Display friendly Name of the Dataset |
| base\_sql | VARCHAR | SQL containing the base procedure to be called to invoke the dataset. The |
| output\_fields | VARCHAR | The result fields that come when the base sql query is executed |
| is\_active | SMALLINT | If the dataset is currently active |
| connection\_ref\_id | INTEGER | Reference ID of the connection being used |

###### picklist\_values (Picklist values)

The table stores actual display values for the front end to display against the more complicated names for various query parameters and attributes shown in the front-end.

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| picklist\_value\_id | INTEGER | Unique identifier assigned to the picklist value |
| picklist\_type | VARCHAR | The type of picklist, i.e. HCP or Patient |
| field\_name | VARCHAR | The field name used in the database |
| value | VARCHAR | The value of the existing field |
| display\_value | VARCHAR | The display value of the field |

###### connection\_ref (Connection Reference)

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| connection\_ref\_id | INTEGER | Uniquely identifies the connection reference |
| connection\_type | VARCHAR | Identifies the type of connection |
| connection\_string | VARCHAR |  |

###### data\_dictionary\_ref (Data Dictionary Reference)

The data model is used for the query layer of the application. It specifies the query parameters as per the data sets available for the customer to query and perform other necessary operations.

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| data\_dictionary\_ref\_id | INTEGER | Unique identifier for the data dictionary entry |
| dataset\_ref\_id | INTEGER | References the |
| field\_name | VARCHAR | The |
| field\_disp\_name | VARCHAR | The display name of the corresponding field |
| description | VARCHAR | Description of the field displayed to the user |
| data\_type | VARCHAR | Data type of the field displayed to the user |
| disp\_data\_type | VARCHAR | User friendly version of the data type displayed to the user |
| field\_values | JSONB | Picklist values or the lookup queries stored and used for populating the options in the drop down menu next to the query parameters |
| inclusion\_flag | SMALLINTEGER | If the query parameter is part of the inclusion criteria |
| exclusion\_flag | SMALLINTEGER | If the query parameter is part of the exclusion criteria |
| export\_flag | SMALLINTEGER | If the query parameter is part of the export flag |
| is\_picklist | SMALLINTEGER | If the query parameter is a picklist or any other type of input field |
| export\_serial | INTEGER | To identify the order of the |
| part\_of\_dataset | VARCHAR | To identify if the field is part of the universe dataset or it is part of transactional data |
| field\_type | VARCHAR | To identify, if the field is a picklist or a |
| data\_dictionary\_ref\_id | INTEGER | Unique identifier for the data dictionary entry |

###### list\_queries (lIST qUERIES)

The table stores the details of all the queries created and saved by the users, including the inclusion and exclusion criteria, among others.

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| list\_query\_id | INTEGER | Unique identifier for the query list. This reference is to display the queries created or saved by the user |
| parent\_query\_id | BIGINT | This is the unique identifier of the parent query created by the user when the original query is modified |
| version | INTEGER | Version of the query if and when modified by the user |
| is\_latest\_version | SMALLINT | Used to indicate if this is the latest version of the query |
| dataset\_ref\_id | INTEGER | Identifier to display which dataset this query id uses to query on |
| query\_type | VARCHAR | Type of query |
| query\_mode | VARCHAR | The mode of querying employed by the user |
| query\_description | VARCHAR | Provision for a short user friendly description of the query that the user has created |
| purpose | VARCHAR | The user friendly input that the user enters as the purpose of generating the query |
| folder\_path | VARCHAR | The Box Folder path the query was exported to |
| channel | VARCHAR | The channel for which the user has created the query |
| campaign\_ref | VARCHAR | The campaign for which the user has created the query |
| tags | VARCHAR | Any other tags added by the user |
| inclusion\_conditions | VARCHAR | The inclusion conditions that the user adds to the query |
| exclusion\_conditions | VARCHAR | The exclusion conditions that the user adds to the query |
| sql\_where | VARCHAR | The user friendly where clause displayed to the user |
| insert\_timestamp | TIMESTAMP WITHOUT TIME ZONE | Indicates the time when the request was created into the table without any time zone details |
| rule\_inclusions | VARCHAR | The inclusion criteria as provided by the user so that stored in a format for the query builder to use |
| rule\_exclusions | VARCHAR | The exclusion criteria as provided by the user so that stored in a format for the query builder to use |
| comments | VARCHAR | Comments if any added by the user |
| created\_by | INTEGER | User ID for the user who has created the query |

###### query\_activity\_hist (query activity history)

The table stores all the details of modifications to saved queries made by users, including edits, the export of lists, share of questions modifications made.

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| query\_hist\_id | INTEGER | Query identifier of the previous version of the query before modification |
| list\_query\_id | BIGINT | Unique identifier of the query |
| parent\_query\_id | BIGINT | Identifier of the parent query of this query |
| user\_id | BIGINT | Unique identifier of the user who created the query from the users table |
| activity\_type | VARCHAR | The activity performed by the user |
| comment | VARCHAR | Comment on the activity if any |
| activity\_timestamp | TIMESTAMP WITHOUT TIME ZONE | Time when the activity occurred |

###### query\_shared\_detail

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| query\_shared\_id | INTEGER | Unique identifier of the shared activity |
| shared\_by\_user\_id | BIGINT | Unique identifier of the user who shared the query |
| shared\_to\_user\_id | BIGINT | Unique identifier of the user to whom the query was shared |
| list\_query\_id | BIGINT | Unique identifier of the shared query |

###### user\_permissions

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| id | INTEGER | Unique identifier of the record |
| user\_id | INTEGER | Unique identifier of the user who was assigned the role |
| permission\_id | INTEGER | Unique identifier of the permission for which the user was assigned the role |
| role\_id | INTEGER | Unique identifier of the roles that are assigned to the user |

###### users

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| user\_name | VARCHAR | Unique username of the user being authorized to use the application |
| first\_name | VARCHAR | First name of the user |
| last\_name | VARCHAR | Last name of the user |
| email | VARCHAR | Email address of the user |
| pwd | VARCHAR | Password assigned to the user in encrypted format |
| is\_active | SMALLINT | Used to indicate if the user is still active |
| user\_name | VARCHAR | Unique username of the user being authorized to use the application |

## **HCP-Level Schema**

###### Account\_ref (Account reference)

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Account\_Id | BIGINT | Uniquely identifies the CLMS user account |
| Account\_Type | VARCHAR | Uniquely identifies the user account type |
| Account\_Id | VARCHAR | Uniquely identifies the user account |
| Account\_Name | VARCHAR | Name of the account |
| pwd | VARCHAR | User account password |
| DEA\_ID | VARCHAR |  |
| HIN\_ID | VARCHAR |  |
| Status | VARCHAR |  |
| INSERT\_TIMESTAMP | TIMESTAMP | Time of account insertion into the table without time zone details |
| UPDATE\_TIMESTAMP | TIMESTAMP | Time when the account was last updated without time zone details |

###### Affiliation\_ref (Affiliation reference)

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| zip | BIGINT | Zip code of the affiliation reference |
| city | TEXT | City of the affiliation reference |
| state | TEXT | State of the affiliation reference |
| territory\_id | TEXT | Identifies uniquely the territory of the affiliation reference |
| region\_id | TEXT | Uniquely identifies the region of the affiliation reference |
| region\_name | TEXT | Name of the region |
| district\_id | TEXT | Uniquely identifies the district of the affiliation reference |
| district\_name | TEXT | Name of the district |
| team | TEXT | Identifies the team |
| file\_name | TEXT |  |
| load\_date | TEXT |  |

###### Affiliation\_Anchor

This table shows the various affiliations of the HCP to parent accounts, parent institutions and anchors, sales teams, territories and regions

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Contact\_Id | BIGINT | Unique identifier for the HCP |
| CLMS\_Account\_Id | BIGINT | The unique identifier assigned by Veeva to the parent account of the HCP. One HCP can have multiple parent accounts |
| CLMS\_Anchor\_Id | BIGINT | The unique identifier assigned by Veeva to the parent anchor of the HCP. One account can have multiple parent anchors |
| Account\_Name | VARCHAR | The name of the parent account |
| Anchor\_Name | VARCHAR | The name of the parent anchor |
| territory\_id | TEXT | The territory to which the HCP, or its parent account belongs. One HCP can be tagged to multiple territories if they appear on the target lists of more than one sales teams |
| territory\_name | TEXT | The name of the territory to which the HCP or its parent account belongs. One HCP can be tagged to multiple territories if they appear on the target lists of more than one sales teams |
| team | TEXT | The sales team for which the HCP, or its parent account or its parent anchor is a target |
| region\_id | TEXT | The unique identifier of the region to which the territory belongs. The region names are specific to the names of the sales teams |
| region\_name | TEXT | The name of the region to which the territory belongs. The region names are specific to the names of the sales teams |

###### Brand

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Brand\_id | BIGINT | Uniquely identifies the brand |
| Brand\_name | VARCHAR | Name of the brand |
| Therapeutic\_Area | VARCHAR | Identifies the therapeutic area |
| INSERT\_TIMESTAMP | TIMESTAMP | Indicates the time when the brand was inserted into the table without the time zone details |
| UPDATE\_TIMESTAMP | TIMESTAMP | Indicates the time when the brand was updated into the table without the time zone details |
| disp\_brand\_name | VARCHAR | Brand name displayed to users |

###### campaign\_acttivity

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Campaign\_Activity\_Id | BIGINT | Campaign activity’s unique identifier |
| CLMS\_Campaign\_Id | BIGINT | Campaign’s unique identifier |
| CLMS\_Brand\_id | INTEGER | Uniquely identifies the brand |
| CLMS\_Contact\_Id | BIGINT | Identifies consumer’s contact |
| CLMS\_Vendor\_Id | INTEGER | Identifies vendor |
| Activity\_Date | DATE | Date of the campaigning activity |
| Activity\_Timestamp | TIMESTAMP | Indicates the time of promotional activity without time zone details |
| Channel | VARCHAR | Indicates the channel |
| Sent\_Flag | VARCHAR | Indicates if the customer was sent an email |
| Engaged\_Flag | VARCHAR | Indicates if the customer was engaged by an email |
| sales\_rep | VARCHAR | Name of the sales representative |
| INSERT\_TIMESTAMP | TIMESTAMP | WITHOUT TIMEZONE |

###### 

###### campaign\_REF

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Campaign\_Id | BIGINT | Uniquely identifies the campaign for HCP into CLMS |
| Campaign\_Id | VARCHAR | Uniquely identifies the campaign for HCP |
| Campaign\_Code | VARCHAR | Code of the campaign |
| Campaign\_Name | VARCHAR | Name of the campaign |
| Campaign\_Type | VARCHAR | Type of the campaign |
| Campaign\_Description | VARCHAR | Describes the promotional campaign |
| Currency\_Iso\_Code | VARCHAR |  |
| Channels | VARCHAR | Communication channels included |
| Tactics | VARCHAR | Tactics included |
| Budgeted\_Cost | REAL | Total budgeted cost |
| Expected\_Response | REAL | The expected response by the campaign |
| Expected\_Revenue | REAL | The expected response generated by the campaign |
| Campaign\_Start\_Date | DATE | The date when the campaign started |
| Campaign\_End\_Date | DATE | The date when the campaign ended |
| INSERT\_TIMESTAMP | TIMESTAMP | Indicates the time of insertion into the table without any time zone details |
| UPDATE\_TIMESTAMP | TIMESTAMP | Indicates the time of updation into the table without any time zone details |

###### ccpa\_REQUESTS

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| clms\_ccpa\_request\_id | BIGINT | Uniquely identifies the CCPA request |
| clms\_contact\_id | BIGINT | Unique identifier for HCP/patient contact |
| request\_queue\_ref\_id | VARCHAR | Uniquely identifies the CCPA request queue |
| date\_created | TIMESTAMP | Indicates the date and time when the CCPA request was created (without the time zone details) |
| date\_updated | TIMESTAMP | Indicates the date and time when the CCPA request was last updated (without the time zone details) |
| date\_completed | TIMESTAMP | Indicates the date and time when the CCPA request was completed (without the time zone details) |
| requestor\_type | VARCHAR | Identifies the type of requestor |
| requestor\_subtype | VARCHAR | Identifies the sub-type of requestor |
| request\_type | VARCHAR | Identifies the type of requestor |
| npi\_id | VARCHAR | NPI identifier for the requestor |
| first\_name | VARCHAR | Identifies the first name of requestor |
| last\_name | VARCHAR | Identifies the last name of requestor |
| email | VARCHAR | Identifies the email address of requestor |
| address | VARCHAR | Identifies the address of requestor |
| zip\_code | VARCHAR | Identifies the zip code of requestor |
| country | VARCHAR | Identifies the country of requestor |
| city | VARCHAR | Identifies the city of requestor |
| state | VARCHAR | Identifies the state of requestor |
| phone | VARCHAR | Phone number of the requestor |
| is\_california\_resident | VARCHAR | Indicates the if requestor is a California resident |
| status | VARCHAR |  |
| insert\_timestamp | TIMESTAMP | Indicates the if requestor is a California resident |
| update\_timestamp | TIMESTAMP | Indicates the if requestor is a California resident |

###### cONSENT\_hISTORY

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Consent\_History\_Id | BIGINT | Uniquely identifies an HCP’s consent history ID |
| CLMS\_Contact\_Id | BIGINT | Unique identifier for HCP contact |
| CLMS\_Brand\_Id | INTEGER | Unique identifier for the brand |
| CLMS\_Campaign\_Id | BIGINT | Unique identifier for the promotional campaign |
| CLMS\_Vendor\_Id | INTEGER | Unique identifier for the vendor |
| Consent\_Date | DATE | Indicates the date of the HCP’s consent obtained |
| Consent\_Timestamp | TIMESTAMP | Indicates the time when the consent obtained without any time zone details |
| Source\_Channel | VARCHAR | Indicates the source channel of campaigning |
| Pref\_Channel | VARCHAR | Indicates the preferred channel of campaigning |
| Opt\_In\_Out\_Category | VARCHAR | Identifies the categories of opt-in and opt-out |
| Opt\_In\_Out\_Type | VARCHAR | Identifies the type of opt-in and opt-out |
| Opt\_In\_Out\_Ind | VARCHAR |  |
| INSERT\_TIMESTAMP | TIMESTAMP | Indicates the time of consent insertion into the table without any time zone details |
| UPDATE\_TIMESTAMP | TIMESTAMP | Indicates the time of consent update into the table without any time zone details |

###### 

###### cONSENT\_SUMMARY

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Contact\_Matching\_Id | BIGINT |  |
| CLMS\_Contact\_Id | BIGINT |  |
| clms\_brand\_id | INTEGER |  |
| channel | VARCHAR |  |
| third\_party | VARCHAR |  |
| opt\_in\_status | VARCHAR |  |
| batch\_run\_id | BIGINT |  |
| insert\_timestamp | TIMESTAMP | WITHOUT TIME ZONE |
| update\_timestamp | TIMESTAMP | WITHOUT TIME ZONE |

###### 

###### cONTACT\_MATCHING

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Contact\_Matching\_Id | BIGINT |  |
| CLMS\_Contact\_Id | BIGINT |  |
| Source | VARCHAR |  |
| Source\_Type | VARCHAR |  |
| Source\_Ref | VARCHAR |  |
| First\_Name | VARCHAR |  |
| Middle\_Name | VARCHAR |  |
| Last\_Name | VARCHAR |  |
| Salutation | VARCHAR |  |
| Suffix | VARCHAR |  |
| Profressional\_Suffix | VARCHAR |  |
| Professional\_Type | VARCHAR |  |
| Primary\_Speciality | VARCHAR |  |
| Secondary\_Speciality | VARCHAR |  |
| Gender | VARCHAR |  |
| YOB | DOUBLE PRECISION |  |
| Weight | VARCHAR |  |
| Email | VARCHAR |  |
| Email2 | VARCHAR |  |
| Email3 | VARCHAR |  |
| Email4 | VARCHAR |  |
| Email5 | VARCHAR |  |
| Email6 | VARCHAR |  |
| Email7 | VARCHAR |  |
| Email8 | VARCHAR |  |
| Email9 | VARCHAR |  |
| Email10 | VARCHAR |  |
| Address\_Line1 | VARCHAR |  |
| Address\_Line2 | VARCHAR |  |
| Address\_Line3 | VARCHAR |  |
| City | VARCHAR |  |
| Region | VARCHAR |  |
| Country | VARCHAR |  |
| V\_ID | VARCHAR |  |
| NPI\_ID | VARCHAR |  |
| IMS\_ID | VARCHAR |  |
| ME\_ID | VARCHAR |  |
| DEA\_ID | VARCHAR |  |
| AMA\_ID | VARCHAR |  |
| Master\_Flag | VARCHAR |  |
| Is\_Valid\_Record | SMALLINT |  |
| Sent\_To\_MasteringSystem | VARCHAR |  |
| Sent\_To\_MasteringSystem\_Timestamp | TIMESTAMP WITHOUT TIME ZONE |  |
| Recd\_From\_MasteringSystem | VARCHAR |  |
| Recd\_From\_MasteringSystem\_Timestamp | TIMESTAMP WITHOUT TIME ZONE |  |
| INSERT\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE |  |
| UPDATE\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE |  |
| POSTAL\_CODE | VARCHAR |  |

###### 

###### cONTACT\_rEF

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Contact\_Id | BIGINT | Uniquely identifies the HCP’s contact into CLMS |
| Contact\_Id | VARCHAR | Uniquely identifies the HCP’s contact |
| Contact\_Src | VARCHAR | Contact source |
| First\_Name | VARCHAR | First name of the contact |
| Middle\_Name | VARCHAR | Middle name of the contact |
| Last\_Name | VARCHAR | Last name of the contact |
| Salutation | VARCHAR | Salutation to the name |
| Suffix | VARCHAR | Suffix to the name (if any) |
| Professional\_Suffix | VARCHAR | Professional suffix to the name |
| Professional\_Type | VARCHAR |  |
| Primary\_Speciality | VARCHAR | Primary speciality of the HCP |
| Secondary\_Speciality | VARCHAR | Secondary speciality of the HCP |
| Gender | VARCHAR | Gender of the HCP |
| YOB | DOUBLE PRECISION | Birth year of the HCP |
| Weight | VARCHAR | Weight of the HCP (in ?) |
| Email | VARCHAR | Primary email address of the HCP |
| Email2 | VARCHAR | Secondary email address of the HCP |
| Email3 | VARCHAR |  |
| Email4 | VARCHAR |  |
| Email5 | VARCHAR |  |
| Email6 | VARCHAR |  |
| Email7 | VARCHAR |  |
| Email8 | VARCHAR |  |
| Email9 | VARCHAR |  |
| Email10 | VARCHAR |  |
| Address\_Line1 | VARCHAR | First line of the HCP address |
| Address\_Line2 | VARCHAR | Second line of the HCP address |
| Address\_Line3 | VARCHAR | Third line of the HCP address |
| City | VARCHAR | City of the HCP |
| Region | VARCHAR | Region of the HCP |
| Postal\_Code | VARCHAR | Zip code of the HCP |
| Country | VARCHAR | Country of the HCP |
| V\_ID | VARCHAR |  |
| NPI\_ID | VARCHAR | NPI identifier of the HCP |
| IMS\_ID | VARCHAR |  |
| ME\_ID | VARCHAR |  |
| DEA\_ID | VARCHAR |  |
| AMA\_ID | VARCHAR |  |
| Screen\_Out\_Ind | VARCHAR |  |
| INSERT\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE | Identifies the time when the HCP contact was inserted into the table (without time zone details) |
| UPDATE\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE | Identifies the time when the HCP contact was last updated into the table (without time zone details) |
| Territory | VARCHAR | territory of the HCP |

###### 

###### cONTACT\_SEGMENT

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Contact\_Segment\_Id | BIGINT |  |
| CLMS\_Contact\_Id | BIGINT |  |
| Brand\_id | INTEGER |  |
| Segment | VARCHAR |  |
| INSERT\_TIMESTAMP | TIMESTAMP | WITHOUT TIME ZONE |
| UPDATE\_TIMESTAMP | TIMESTAMP | WITHOUT TIME ZONE |

###### 

###### lEAD\_REGISTRATIONS

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Lead\_Id | BIGINT | Uniquely identifies the customer profile |
| CLMS\_Contact\_Id | BIGINT | Uniquely identifies the customer contact |
| CLMS\_Brand\_id | INTEGER | Uniquely identifies the brand to be promoted |
| CLMS\_Vendor\_Id | INTEGER | Uniquely identifies the vendor |
| Lead\_Source | VARCHAR | Source of the profile |
| Lead\_Source\_Ref | VARCHAR | Reference to the profile source |
| Registration\_Date | DATE | Date of the profile registration |
| Registration\_Timestamp | TIMESTAMP | Time of the profile registration (without time zone details) |
| INSERT\_TIMESTAMP | TIMESTAMP | Time of the profile insertion into the table (without time zone details) |
| match\_flag | VARCHAR | Indicates if the profile matches to ? |

###### 

###### VENDOR\_REF

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Vendor\_Id | BIGINT | Uniquely identifies the vendor |
| Vendor | VARCHAR | Name of the vendor |
| Is\_Third\_Party | VARCHAR | Indicates if the vendor is third-party or not |
| disp\_vendor\_name | TIMESTAMP | WITHOUT TIME ZONE |
| is\_engagement\_vendor | BOOLEAN | Indicates if the vendor is an engagement vendor |
| is\_profile\_vendor | BOOLEAN | Indicates if the vendor is a profile vendor |

## **Patient-Level Schema**

###### Brand

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Brand\_id | INTEGER | Unique identifier for brand |
| Brand\_name | VARCHAR | Name of the brand |
| Therapeutic\_Area | VARCHAR | Identifies the therapeutic area |
| INSERT\_TIMESTAMP | TIMESTAMP | Identifies the data and time of brand insertion (without time zone details) |
| UPDATE\_TIMESTAMP | TIMESTAMP | Identifies the data and time when the brand list updated (without time zone details) |
| batch\_run\_id | BIGINT | Batch identifier for the job that populates data into the table |
| disp\_brand\_name | VARCHAR | The brand name used for displaying to the user |

###### 

###### 

###### campaign\_acttivity

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Campaign\_Activity\_Id | INTEGER | Uniquely identifies CMS campaign activity |
| CLMS\_Campaign\_Id | BIGINT | Uniquely identifies CMS campaign |
| CLMS\_Brand\_id | INTEGER | Unique identifier for brand |
| CLMS\_Contact\_Id | BIGINT | Unique identifier for HCP/patient contact |
| CLMS\_Vendor\_Id | INTEGER | Unique identifier for vendor |
| Activity\_Date | DATE | Date of the campaign activity |
| Activity\_Timestamp | TIMESTAMP | Indicates the activity time without any time zone details |
| Channel | VARCHAR | Identifies the campaigning channel |
| Sent\_Flag | VARCHAR | Indicates if the customer was sent an email |
| Engaged\_Flag | VARCHAR | Indicates if the customer was engaged by an email |
| INSERT\_TIMESTAMP | TIMESTAMP | Indicates the time of insertion into the table without any time zone details |
| batch\_run\_id | BIGINT | Batch identifier for the job that populates data into the table |

###### 

###### campaign\_REF

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Campaign\_Id | BIGINT | Uniquely identifies CMS campaign |
| Campaign\_Id | VARCHAR | Uniquely identifies CMS campaign |
| Campaign\_Code | VARCHAR | Identifies the campaign code |
| Campaign\_Name | VARCHAR | Identifies the name of the campaign |
| Campaign\_Type | VARCHAR | Identifies the campaign type |
| Campaign\_Description | VARCHAR | Describes the promotional campaign |
| Currency\_Iso\_Code | VARCHAR |  |
| Channels | VARCHAR | Communication channels included |
| Tactics | VARCHAR | Tactics included |
| Budgeted\_Cost | REAL | Total budgeted cost |
| Expected\_Response | REAL | The expected response by the campaign |
| Expected\_Revenue | REAL | The expected response generated by the campaign |
| Campaign\_Start\_Date | DATE | The date when the campaign started |
| Campaign\_End\_Date | DATE | The date when the campaign ended |
| INSERT\_TIMESTAMP | TIMESTAMP | Indicates the time of insertion into the table without any time zone details |
| UPDATE\_TIMESTAMP | TIMESTAMP | Indicates the time of update into the table without any time zone details |

###### ccpa\_REQUESTS

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| clms\_ccpa\_request\_id | BIGINT | Uniquely identifies the CCPA request |
| clms\_contact\_id | BIGINT | Unique identifier for HCP/patient contact |
| request\_queue\_ref\_id | VARCHAR | Uniquely identifies the CCPA request queue |
| date\_created | TIMESTAMP | Indicates the date and time when the CCPA request was created (without the time zone details) |
| date\_updated | TIMESTAMP | Indicates the date and time when the CCPA request was last updated (without the time zone details) |
| date\_completed | TIMESTAMP | Indicates the date and time when the CCPA request was completed (without the time zone details) |
| requestor\_type | VARCHAR | Identifies the type of requestor |
| requestor\_subtype | VARCHAR | Identifies the sub-type of requestor |
| request\_type | VARCHAR | Identifies the type of requestor |
| first\_name | BYTE | Identifies the first name of requestor |
| last\_name | BYTE | Identifies the last name of requestor |
| email | BYTE | Identifies the email address of requestor |
| address | BYTE | Identifies the address of requestor |
| zip\_code | BYTE | Identifies the zip code of requestor |
| first\_name\_hash | BYTE |  |
| last\_name\_hash | BYTE |  |
| email\_hash | BYTE |  |
| address\_hash | BYTE |  |
| zip\_code\_hash | BYTE |  |
| country | VARCHAR | Identifies the country of the requestor |
| city | VARCHAR | Identifies the city of the requestor |
| state | VARCHAR | Identifies the state of the requestor |
| phone | BYTE | Identifies the phone contact of the requestor |
| is\_california\_resident | VARCHAR | Indicates the if requestor is a California resident |
| status | VARCHAR | Identifies the status of request |
| insert\_timestamp | TIMESTAMP | Indicates the time of request insertion into the table without any time zone details |
| update\_timestamp | TIMESTAMP | Indicates the time of request update into the table without any time zone details |
| batch\_run\_id | BIGINT | Batch identifier for the job that populates data into the table |

###### cONSENT\_hISTORY

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Consent\_History\_Id | INTEGER | Uniquely identifies the patient’s consent history ID |
| CLMS\_Contact\_Id | BIGINT | Unique identifier for patient contact |
| CLMS\_Brand\_Id | INTEGER | Unique identifier for the brand |
| CLMS\_Campaign\_Id | BIGINT | Unique identifier for the promotional campaign |
| CLMS\_Vendor\_Id | INTEGER | Unique identifier for the vendor |
| Consent\_Date | DATE | Indicates the date of the consent obtained |
| Consent\_Timestamp | TIMESTAMP | Indicates the time when the consent obtained without any time zone details |
| Source\_Channel | VARCHAR | Indicates the source channel of campaigning |
| Pref\_Channel | VARCHAR | Indicates the preferred channel of campaigning |
| Opt\_In\_Out\_Category | VARCHAR | Identifies the categories of opt-in and opt-out |
| Opt\_In\_Out\_Type | VARCHAR | Identifies the type of opt-in and opt-out |
| Opt\_In\_Out\_Ind | VARCHAR |  |
| INSERT\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE | Indicates the time of consent insertion into the table without any time zone details |
| UPDATE\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE | Indicates the time of consent update into the table without any time zone details |
| batch\_run\_id | BIGINT | Batch identifier for the job that populates data into the table |

###### cONSENT\_SUMMARY

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| Consent\_Summary\_Id | INTEGER | Uniquely identifies the consent summary |
| CLMS\_Contact\_Id | BIGINT | Uniquely ide |
| clms\_brand\_id | INTEGER |  |
| channel | VARCHAR |  |
| Is\_Third\_Party | VARCHAR |  |
| opt\_in\_status | VARCHAR |  |
| insert\_timestamp | TIMESTAMP | WITHOUT TIME ZONE |
| update\_timestamp | TIMESTAMP | WITHOUT TIME ZONE |
| batch\_run\_id | BIGINT | Batch identifier for the job that populates data into the table |

###### 

###### cONTACT\_MATCHING

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CMS\_Contact\_Matching\_Id | INTEGER |  |
| CLMS\_Contact\_Id | BIGINT |  |
| Source | VARCHAR |  |
| Source\_Type | VARCHAR |  |
| Source\_Ref | VARCHAR |  |
| First\_Name | VARCHAR |  |
| Middle\_Name | VARCHAR |  |
| Last\_Name | VARCHAR |  |
| Salutation | VARCHAR |  |
| Suffix | VARCHAR |  |
| Profressional\_Suffix | VARCHAR |  |
| Professional\_Type | VARCHAR |  |
| Gender | VARCHAR |  |
| YOB | VARCHAR |  |
| Weight | DOUBLE PRECISION |  |
| Email | BYTEA |  |
| Email2 | BYTEA |  |
| Email3 | BYTEA |  |
| Email4 | BYTEA |  |
| Email5 | BYTEA |  |
| Email6 | BYTEA |  |
| Email7 | BYTEA |  |
| Email8 | BYTEA |  |
| Email9 | BYTEA |  |
| Email10 | BYTEA |  |
| Address\_Line1 | BYTEA |  |
| Address\_Line2 | BYTEA |  |
| Address\_Line3 | BYTEA |  |
| City | VARCHAR |  |
| Region | VARCHAR |  |
| Postal\_Code | BYTEA |  |
| Country | VARCHAR |  |
| Validate\_Flag | VARCHAR |  |
| Mastering\_Tmestamp | TIMESTAMP WITHOUT TIME ZONE |  |
| Is\_Valid\_Record | SMALLINT |  |
| INSERT\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE |  |
| UPDATE\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE |  |
| Email\_hash | BYTEA |  |
| First\_Name\_hash | BYTEA |  |
| Last\_Name\_hash | BYTEA |  |
| Address\_Line1\_hash | BYTEA |  |
| Address\_Line2\_hash | BYTEA |  |
| Address\_Line3\_hash | BYTEA |  |
| Postal\_Code\_hash | BYTEA |  |
| Middle\_Name\_hash | BYTEA |  |
| Email2\_hash | BYTEA |  |
| Email3\_hash | BYTEA |  |
| Email4\_hash | BYTEA |  |
| Email5\_hash | BYTEA |  |
| Email6\_hash | BYTEA |  |
| Email7\_hash | BYTEA |  |
| Email8\_hash | BYTEA |  |
| Email9\_hash | BYTEA |  |
| Email10\_hash | BYTEA |  |
| batch\_run\_id | BIGINT | Batch identifier for the job that populates data into the table |

###### 

###### cONTACT\_rEF

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Contact\_Matching\_Id | INTEGER | Uniquely identifies the patient’s contact into CLMS |
| Contact\_Id | VARCHAR | Uniquely identifies the patient’s contact |
| Contact\_Src | VARCHAR | Contact source |
| First\_Name | BYTEA | First name of the contact |
| Middle\_Name | BYTEA | Middle name of the contact |
| Last\_Name | BYTEA | Last name of the contact |
| Salutation | VARCHAR | Salutation to the name |
| Suffix | VARCHAR | Suffix to the name (if any) |
| Profressional\_Suffix | VARCHAR | Professional suffix to the name |
| Professional\_Type | VARCHAR |  |
| Gender | VARCHAR | Gender of the patient |
| YOB | VARCHAR | Birth year of the patient |
| Weight | DOUBLE PRECISION | Weight of the patient (in ?) |
| Email | BYTEA | Primary email address of the patient |
| Email2 | BYTEA | Secondary email address of the HCP |
| Email3 | BYTEA |  |
| Email4 | BYTEA |  |
| Email5 | BYTEA |  |
| Email6 | BYTEA |  |
| Email7 | BYTEA |  |
| Email8 | BYTEA |  |
| Email9 | BYTEA |  |
| Email10 | BYTEA |  |
| Address\_Line1 | BYTEA | First line of the HCP address |
| Address\_Line2 | BYTEA | Second line of the HCP address |
| Address\_Line3 | BYTEA | Third line of the HCP address |
| City | VARCHAR | City of the HCP |
| Region | VARCHAR | Region of the HCP |
| Postal\_Code | BYTEA | Zip code of the HCP |
| Country | VARCHAR | Country of the HCP |
| Screen\_Out\_Ind | VARCHAR |  |
| INSERT\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE | First line of the patient address |
| UPDATE\_TIMESTAMP | TIMESTAMP WITHOUT TIME ZONE | Second line of the patient address |
| Email\_hash | BYTEA |  |
| First\_Name\_hash | BYTEA |  |
| Last\_Name\_hash | BYTEA |  |
| Address\_Line1\_hash | BYTEA |  |
| Address\_Line2\_hash | BYTEA |  |
| Address\_Line3\_hash | BYTEA |  |
| Postal\_Code\_hash | BYTEA |  |
| Middle\_Name\_hash | BYTEA |  |
| Email2\_hash | BYTEA |  |
| Email3\_hash | BYTEA |  |
| Email4\_hash | BYTEA |  |
| Email5\_hash | BYTEA |  |
| Email6\_hash | BYTEA |  |
| Email7\_hash | BYTEA |  |
| Email8\_hash | BYTEA |  |
| Email9\_hash | BYTEA |  |
| Email10\_hash | BYTEA |  |
| batch\_run\_id | BIGINT | Batch identifier for the job that populates data into the table |

###### lEAD\_REGISTRATIONS

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Lead\_Id | INTEGER | Identifies consumer profile ID |
| CLMS\_Brand\_id | INTEGER | Identifies brand |
| CLMS\_Vendor\_Id | INTEGER | Identifies vendor |
| CLMS\_Contact\_Id | BIGINT |  |
| Lead\_Source | VARCHAR |  |
| Lead\_Source\_Ref | VARCHAR |  |
| Registration\_Date | DATE |  |
| Registration\_Timestamp | TIMESTAMP | WITHOUT TIME ZONE |
| INSERT\_TIMESTAMP | TIMESTAMP | WITHOUT TIME ZONE |
| match\_flag | VARCHAR |  |
| batch\_run\_id | BIGINT | Batch identifier for the job that populates data into the table |

###### 

###### 

###### VENDOR\_REF (vendor reference)

|  |  |  |
| --- | --- | --- |
| Field Name | Data Type | Description |
| CLMS\_Vendor\_Id | INTEGER | CLMS vendor identifier |
| Vendor | VARCHAR | Name of the vendor |
| Is\_Third\_Party | VARCHAR | Indicates if the vendor is third party |
| disp\_vendor\_name | TIMESTAMP | Without time zone details |
| is\_engagement\_vendor | BOOLEAN |  |
| is\_profile\_vendor | BOOLEAN |  |