

Concept for a vaccination data ecosystem

April 6th 2022 – Final version, validated by project management committee

Collective work by (in alphabetical order) BFH, FMH, Galenicare, HCI Solutions, Interpharma, MIDATA and pharmaSuisse.

This validated version is openly released.

Table of contents

1. Introduction

- 1.1. Analysis and solution
- 1.2. Principles
- 1.3. Main stakeholders and roles

2. Use cases and Minimal Viable Product (MVP)

- 2.1. Patient user journey
 - 2.1.1 Patient personas
 - 2.1.2 Patient journeys
- 2.2. HP user journey
- 2.3. Data entry by patient
- 2.4. Data entry by HP
- 2.5. Patient onboarding
 - 2.5.1. Patient registration by HP
 - 2.5.2. Patient registration via patient app
- 2.6. Data validation by HP
- 2.7. Notification by CDS
- 2.8. Patient account lifecycle management
 - 2.8.1. Account creation
 - 2.8.2. Account ID / email change
 - 2.8.3. Password change
 - 2.8.4. Data export
 - 2.8.5. Data deletion
 - 2.8.6. Quit vaccination booklet ecosystem
 - 2.8.7. MIDATA patient account deletion
- 2.9. HP account lifecycle management
 - 2.9.1. HP identity verification
 - 2.9.2. HP onboarding and authentication
 - 2.9.3 MIDATA HP login
 - 2.9.4. MIDATA HP account editing
 - 2.9.5. MIDATA HP account deletion
 - 2.9.6. Generation of HP personal QR code/personal code
- 2.10. Search/authorize/linking patient-HP
 - 2.10.1. Patient use case
 - 2.10.2. HP use case

3. Data

- 3.1. Data model

- [3.1.1. Entities](#)
 - [3.2. FHIR format](#)
 - [3.2.1. CH VACD](#)
 - [3.2.2. Relevant FHIR resources](#)
- [4. Identification and authentication](#)
 - [4.1. HP ID and login](#)
- [5. Architecture & API](#)
 - [5.1. General architecture and components list](#)
 - [5.2. Support of FHIR API and concepts](#)
 - [5.2.1. General FHIR resource interactions](#)
 - [5.2.1.1. Requests](#)
 - [5.2.1.2. Responses](#)
 - [5.2.1.3. Response codes](#)
 - [5.2.2. Common functionalities](#)
 - [5.2.2.1. Search patient](#)
 - [5.2.2.2. Retrieve data](#)
 - [5.2.2.3. Adding data](#)
 - [5.2.2.4. Updating data](#)
 - [5.2.2.5. Deleting data](#)
 - [5.3. Patient app to MIDATA](#)
 - [5.3.1. Register new patient](#)
 - [5.3.2. Add new data record](#)
 - [5.3.3. Authorize HP \(Consent\)](#)
 - [5.3.3.1. QR code](#)
 - [5.3.3.2. Personal code](#)
 - [5.3.3.3. Creating the consent](#)
 - [5.3.4. Send reminders to patients](#)
 - [5.4. HP app to MIDATA](#)
 - [5.4.1. Register a new patient](#)
 - [5.4.2. Add new data record](#)
 - [5.4.3. Validate existing data record](#)
 - [5.5. HP authentication services](#)
 - [5.5.1. Register HP](#)
 - [5.6. Patient app to CDS](#)
 - [5.7. HP app to CDS](#)
- [6. Legal](#)
 - [6.1. Relationship patient app owner to MIDATA](#)
 - [6.1.1. The MIDATA platform as a secure patient-centric backend](#)
 - [6.1.2. Relationship patient app owner and service provider to MIDATA](#)
 - [6.2. Relationship patient to patient app provider](#)

- [6.3. Relationship patient to MIDATA](#)
- [6.4. Relationship HP app owner and HP to MIDATA](#)
- [6.5. Relationship patient app provider to CDSS provider](#)
- [6.6. Relationship patient/HP to CDSS provider](#)
- [6.7. Relationship HP app operator to CDSS operator](#)
- [6.8. Relationship HP to HP app operator](#)
- [6.9. Relationship HP app operator to HP eID operator](#)
- [6.10. Relationship HP to HP eID operator](#)
- [6.11. Alternative organizational and legal setup](#)

[7. Security by design](#)

- [7.1. General security principles](#)
- [7.2. Logins \(identification, authentication\)](#)
 - [7.2.1. Lifecycle management](#)
- [7.3. Autorisation for HP](#)
- [7.6. Data access management](#)
- [7.7. Data encryption](#)
- [7.8. Network security](#)
- [7.9. Log files / Audit logs](#)
- [7.10. Testing](#)
- [7.11. Security audit](#)

[8. Operations](#)

- [8.1. General considerations](#)
- [8.2. Release management](#)
- [8.3. Reporting: indicators and statistics](#)
- [8.4. Service Level Agreement](#)
- [8.5. First level support for all components](#)
- [8.6. Second level support for all components](#)
- [8.7. Monitoring, alerting and escalation procedure](#)
- [8.8. Data recovery plan](#)

[9 Categorizations of functionalities](#)

- [9.1 Not in MVP, optional features](#)
 - [9.1.1 User journey "import vaccination data by HP"](#)
 - [9.1.2 Test data](#)
 - [9.1.3 CDSS for patients](#)
 - [9.1.4 Notification by CDS](#)
 - [9.1.5 Patient ID with Trust ID or SwissID](#)
 - [9.1.6 External signature of validated records](#)

[10. Glossary](#)

[11. Appendix](#)

- [11.1 Legal relationship split by actors for a better readiness](#)

[11.2 Requirements and existing eIDs for HP](#)

[11.3 Example of a SAML assertion contained in a HIN token](#)

[11.4 Terms and conditions of the solution providers](#)

Note for the reader:

In the text both gender forms male and female are always meant, for clarity the male form will be used, meaning both.

The term *customer* might be preferred to patient in the context of a pharmacy visit, but for this project can be interchanged with the term *patient*. In general the term *patient* will be preferred.

1. Introduction

The collapse and liquidation of *meineimpfungen.ch* has two main consequences:

- There has been no corresponding offer for several months, although the need among patients and health professionals is undisputed and the demand will increase, also induced by Covid-19.
- All vaccinations that were documented in the old platform are no longer accessible for the time being; online access to the data (which still exists as an archive) is therefore no longer possible.

1.1. Analysis and solution

At the FOPH and eHealth Suisse, the idea has arisen to use the EPR (EPD in German) as a catch-all for the vaccination data.

In view of the current developments in the area of EPR and the lack of a legal basis to manage dynamic data in the master communities, it seems that the realization of an EPR-based solution in a timely manner (within 2022) for vaccinations with an integrated vaccination recommendation algorithm is improbable.

Prof. Serge Bignens from the Bern University of Applied Sciences, Institute for Medical Informatics, got involved to initiate a rescue solution for *meineimpfungen.ch*.

The initial focus was on saving the archived data.

In the meantime, several stakeholders (details below) support this initiative ideally, financially and/or through in-kind contributions; the financing of the first stage is largely secured.

The legal situation regarding data access to the "old" data is completely unclear; the FOPH and the FDPIC have been approached several times, but both agencies did not show interest.

Due to the unclear situation regarding the old data, a concept plus a 2-phase implementation is planned:

- Concept: writing of this report to document uses cases, security by design, governance, operation, legal and communication.
- Phase 1: development of a new web platform that is completely independent of the old system and that reproduces the functional scope of *meineimpfungen.ch* as far as possible.

- Phase 2: once the legal situation regarding access to the old data has been clarified at a later date, citizens will be offered the option of integrating this data from a XML file into the new platform.

1.2. Principles

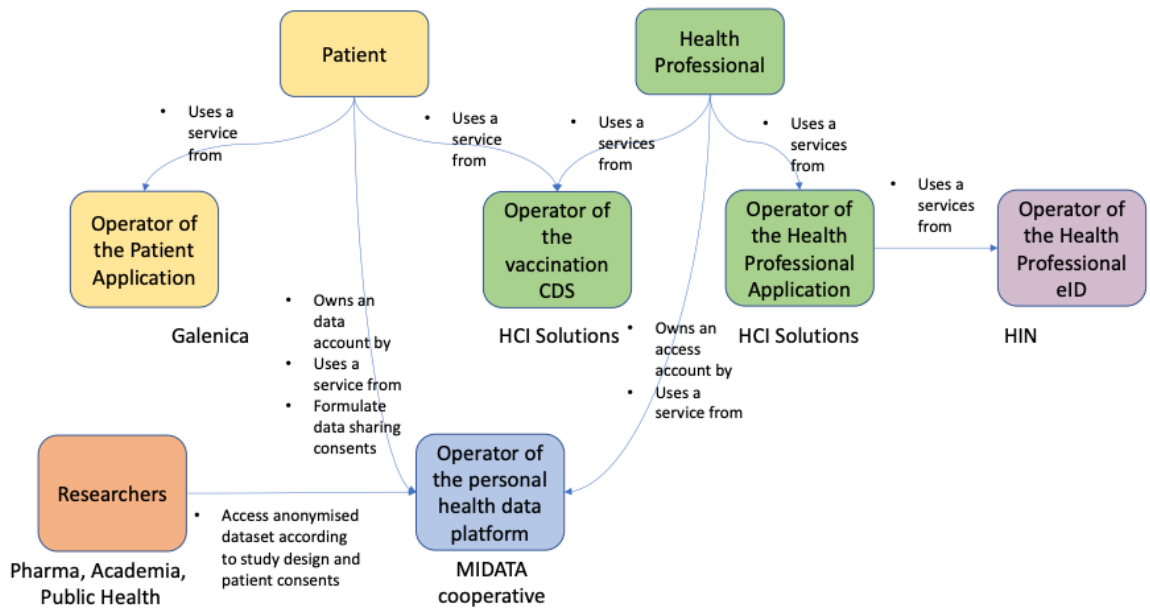
The following principles have been leading the concept of the solution:

- Broad-based dialog (service providers, academia, industry, society)
- Data sovereignty is with the citizens
- Data protection is in the foreground, lessons learned from the previous platform are taken into account
- The solution should empower patients and give them direct access to best validated information on recommended vaccinations, leading to a better protection of the population against several diseases.
- The secondary use of structured longitudinal data, provided patient gives explicit consent to it, will be facilitated
- This concept document will be disclosed
- Transparency regarding the roles of stakeholders in development, operation and funding
- All interfaces with standard API for transport and semantics
- CH-HL7-FHIR vaccination exchange format is supported
- Open platform for an open ecosystem
- Use of proven components existing in CH
- Possible connection and interaction with EPD as soon as the regulation and the interfaces allow it.

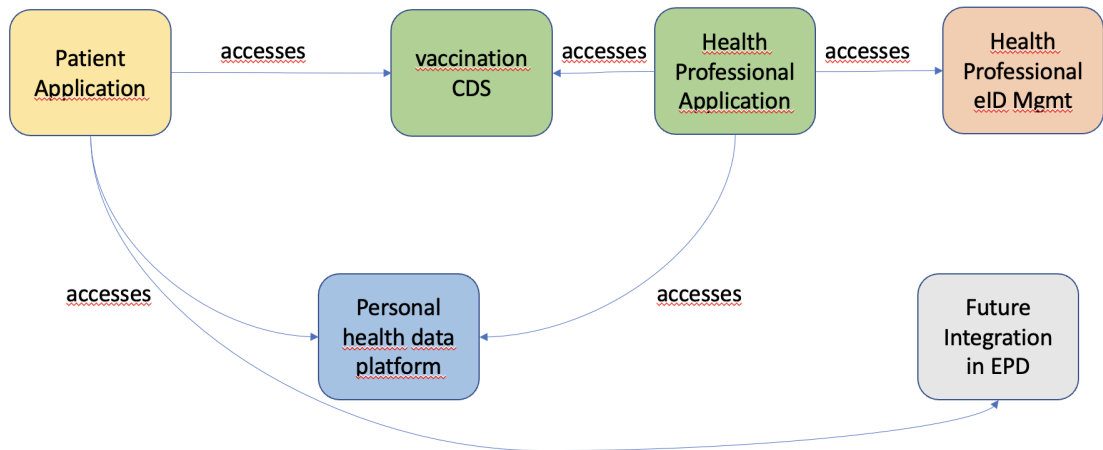
1.3. Main stakeholders and roles

Stakeholder	Role
Committed	
BFH	Specifications, data semantics, support
MIDATA	Data storage, incl. consent management
HCI Solutions, Galenicare	Programming of rules and regulations (medical device) and GUI B2C module: web app for patients
pharmaSuisse	Patronage
FMH	Patronage
Interpharma	Patronage
Interpharma members	Financing
Contacted	
HIN	HP identity provider
OFAC, ELCA, ISS	Hosting
Other industry partner	Financing
Health insurer	Financing, distribution

The two following schemas illustrate the actors and the software components:



Schema 1: Actors & their relationships.



Schema 2: Software components & their relationships.

2. Use cases and Minimal Viable Product (MVP)

2.1. Patient user journey

Three typical patient personas are described below. And a series of customer/patient journeys required for a convenient market solution.

2.1.1 Patient personas

Sarah Meyer, 42



Marketing Manager
(80%)

Married, boy (8)

Mobile services as first
choice

Has no vaccination
dossier. Her husband
has a
meineimpfungen.ch (old)
dossier

**“I appreciate quality
services adapted to my
life trend.”**

Bio: *Very busy working and managing the family. Her husband works 100%. She manages family and job. Lives in a small village 15 minutes away from the city and working area.*

Life Style: *Career, family, friends and her hobbies are most important for her. A volleyball player with tournaments on weekends.*

Love vacation and diving with her family. Hiking in the mountains and spending time in nature with her son.

Needs:

- *More free time to enjoy life*
- *Less administration time*
- *Flexibility in appointments*
- *Rapid access to quality services and advices*
- *Mobile services as first choice*
- *Access to all data online (mobile if possible)*

Pains:

- *Manages all in household*
- *Manages all appointments of house including doctors' visits, medication and health care activities*
- *Difficult to manage strict open hours for services due to full timetable*

Lucy Schneider,
25



Sales Person (100%)

Lives with her boyfriend

Only mobile services
Decides to create a
vaccination dossier
since she can manage it
on her mobile

**“I need more than 24
hours a day”**

Bio: *In early career phase. Starting to plan her own life. Lives and works in the city. No car, only public transports. Lots of expenses moving out of her parents. Low budget available. Credit to buy furniture.*

Life Style: *Friends, friends and friends. Going out all the time, enjoying after work apéro, weekend parties, vacations overseas. 3 Zumba dancing classes a week.*

Sees her parents twice a month, in a nearby village. Her older sister, married with 2 small kids lives nearby the parents. Spent a few hours with nephews once a while and babysits to allow her sister a night out once a while.

Needs:

- *Time for everyone, no time for her*
- *Little or no organization in her life, needs last minute services*
- *Flexibility in appointments, no quality needed*
- *Rapide access to services*
- *Everything should be possible on mobile*

Pains:

- *Never plans in advance*
- *Always late on schedule*
- *Follows the trends on social networks*
- *Very healthy, no family doctor*

Peter Steiner, 55



Top Management (100%)

Married, 2 children (18 and 21)

Mobile services or online access are a must

Has an old vaccination dossier on paper and PDF

“Convenient service and quality advice”

Bio: Top manager career. With international travel. Successful and busy. Find the equilibrium between family and career.

In shape, sportive and healthy lifestyle.

Life Style: Very busy during weekdays, mostly free for family and hobbies on weekends. Enjoys long distance vacations in Africa and Asia.

Needs:

- *Easy and flexible access to health care service. Being in good health and minimum contact with doctors*
- *Looking for quality service independent of cost if convenient to his needs*
- *Needs online access (mobile or web)*

Pains:

- *Delay in health care service. Doctors' appointments are more and more long if not urgent*
- *Very busy professional agenda, weekends are his ideal healthcare appointments that only pharmacies can provide*

2.1.2 Patient journeys

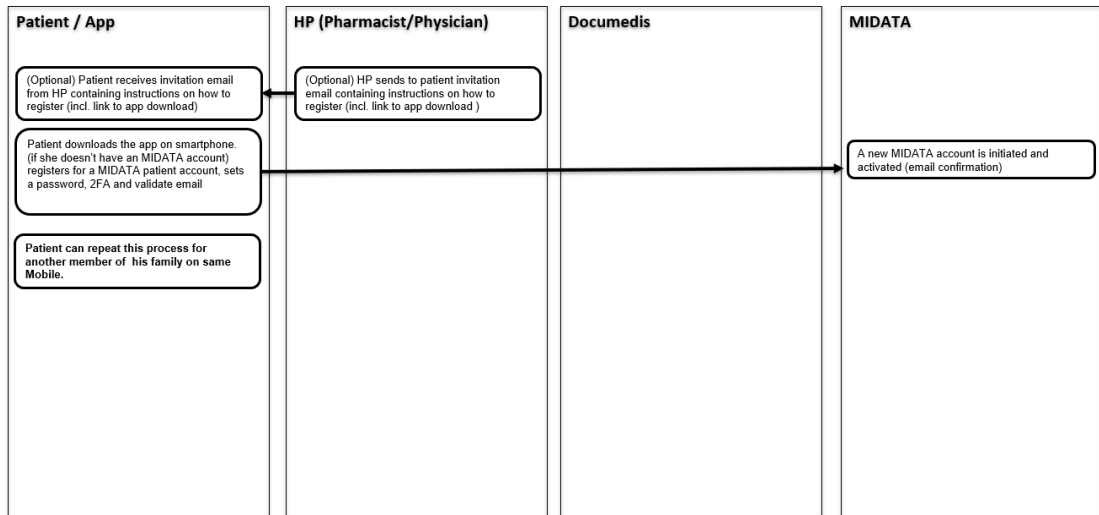
User journey 1

Self registration and authorisation

User journey 1a

Register for an electronic vaccination booklet (self-registration)

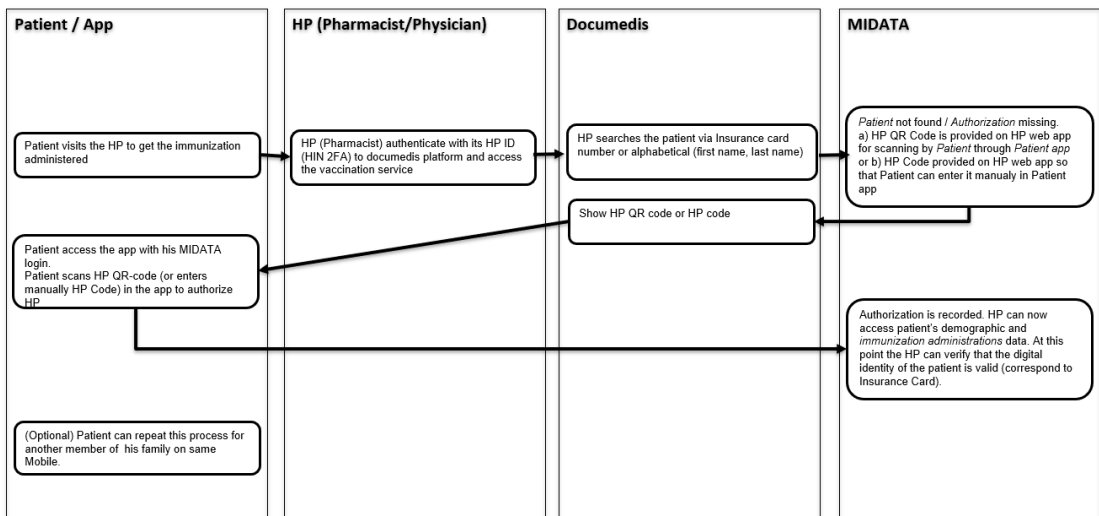
Patient proceeds with self registration for a vaccination booklet.



User journey 1b

Register for an electronic vaccination booklet (authorisation)

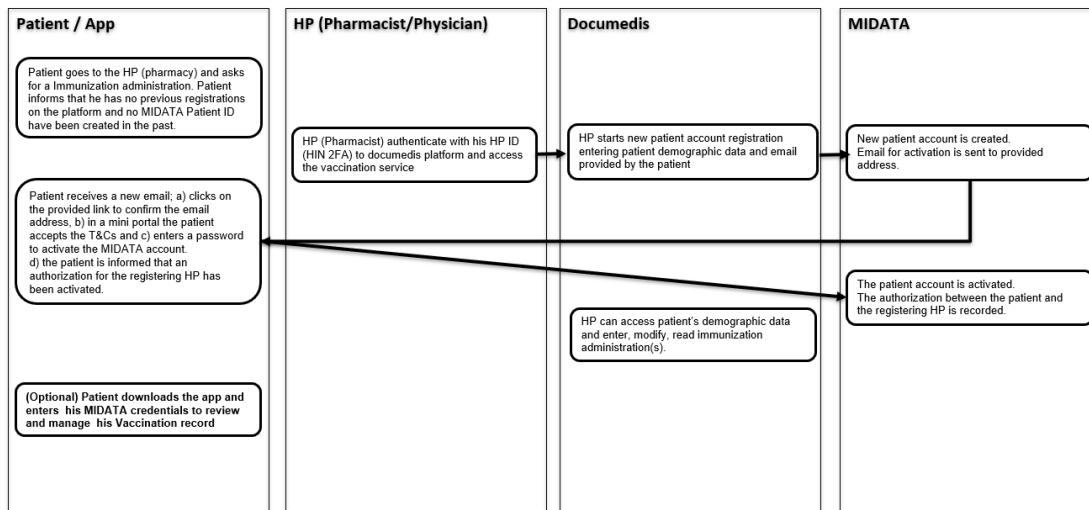
Patient authorizes HP to access his vaccination booklet.



User journey 2

Register for an electronic vaccination booklet (registration by HP + authorization)

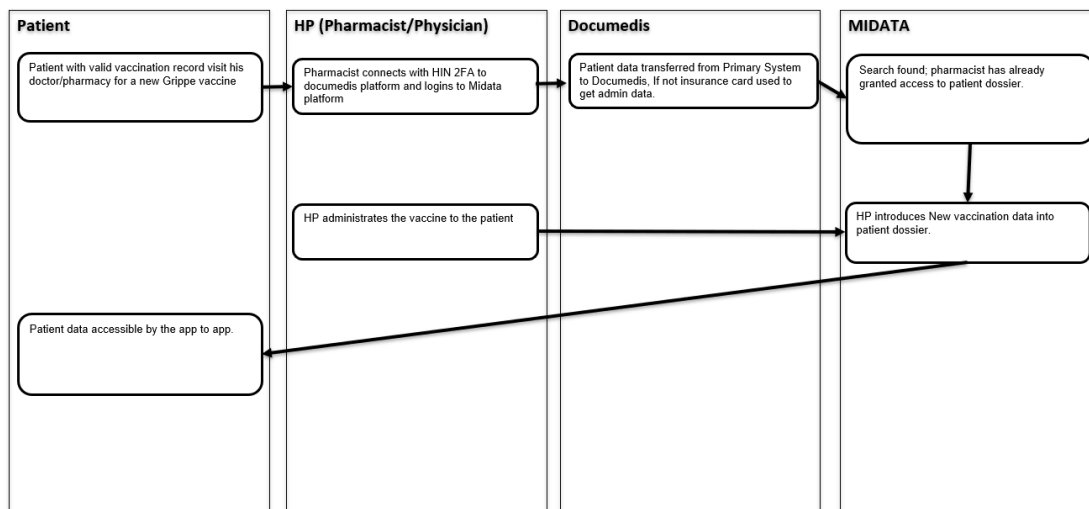
Patient asks his HP to register him for a vaccination booklet and give the HP authorisation.



User journey 3

Patient visit HP for a new vaccination administration

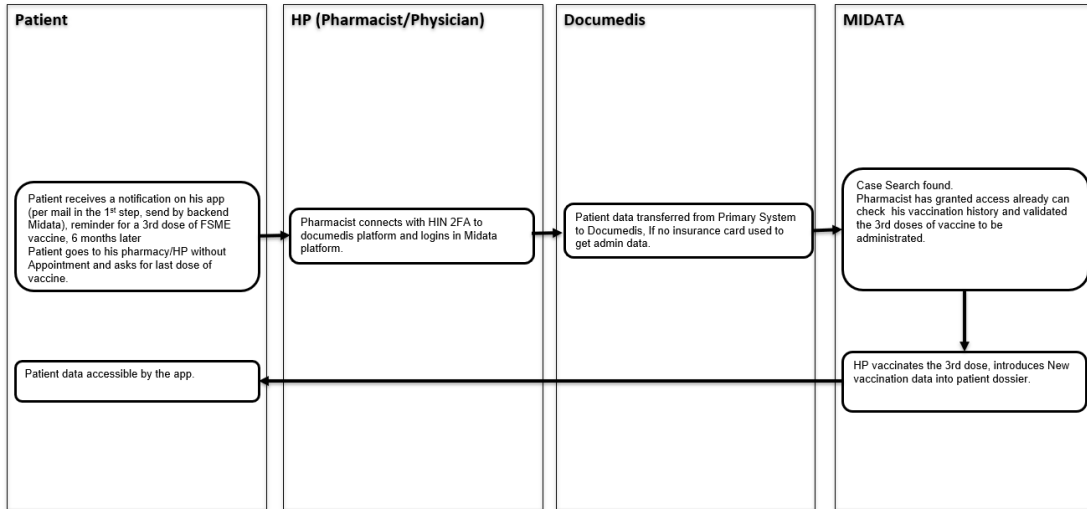
Patient visits his HP with a valid vaccination record and requests for a new vaccination.



User journey 4

Reminder for a next dose of vaccine

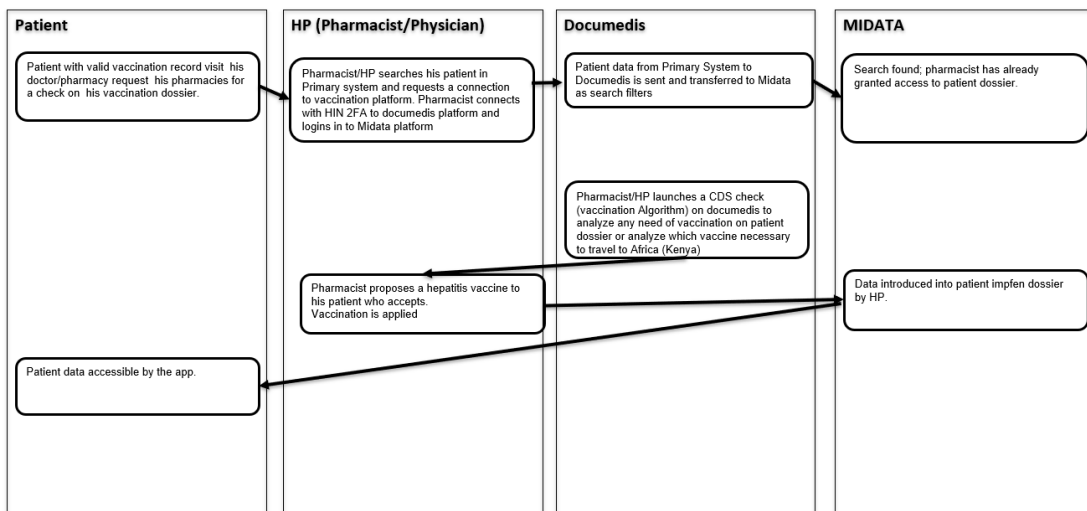
Patient receives a reminder on his app for his next dose of TBE (FSME) vaccine.



User journey 5

Patient requests or HP proposes a CDS check for new vaccine in the pharmacy/HP

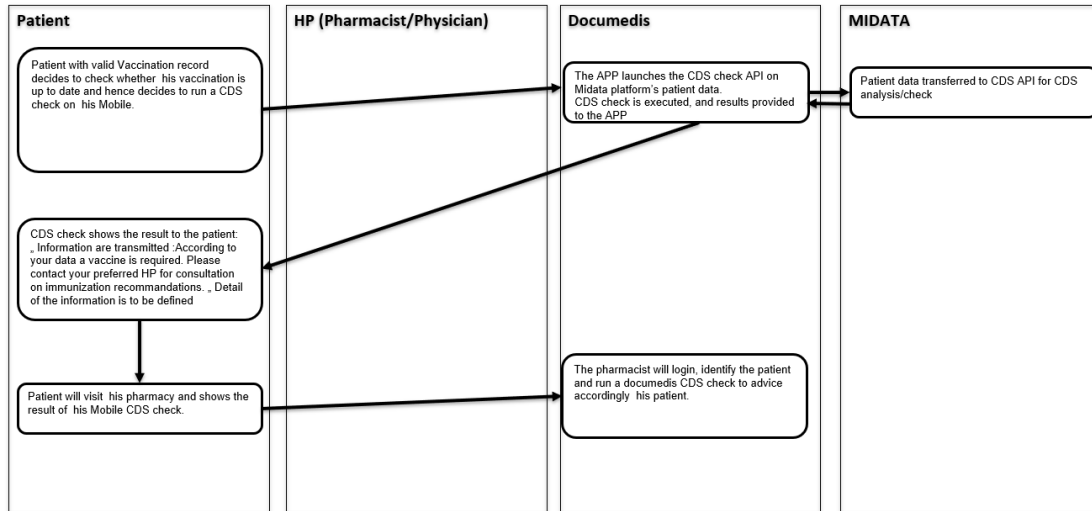
Patient with a valid vaccination record visits his pharmacy and receives a CDS check on his immunization record by the HP to identify any new immunizations needed.



User journey 6

Patient requests a CDS check on his mobile app

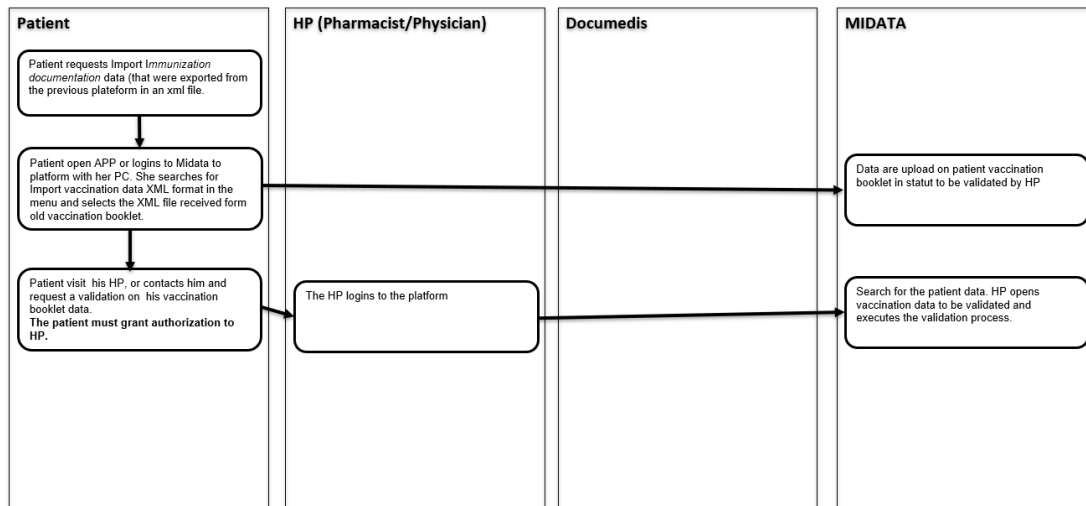
Patient with a valid vaccination record requests a CDS check on his immunization dossier on his mobile.



User journey 7

Import XML data from old meineimpfungen.ch platform

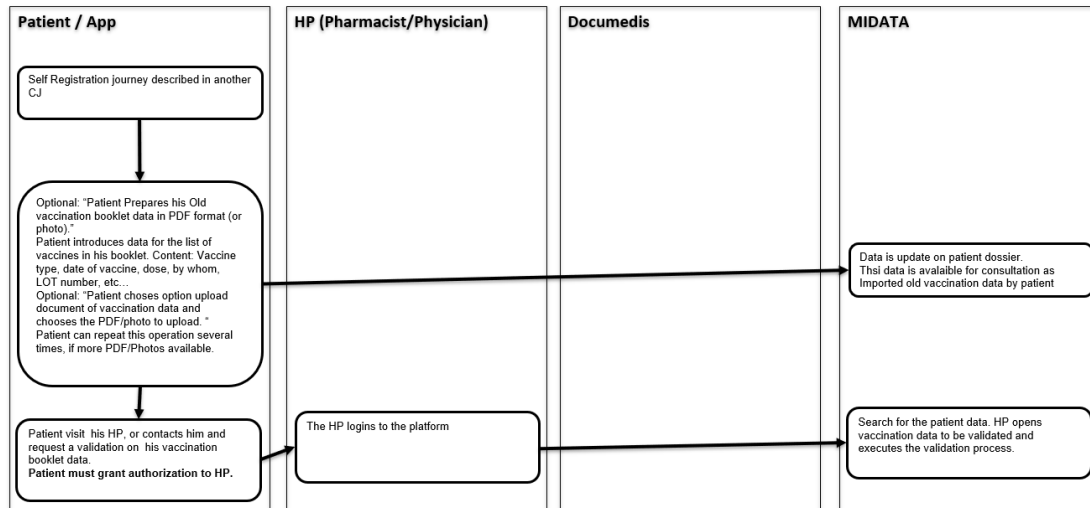
Patient imports his old vaccination record with the XML file of the meineimpfungen.ch dossier and asks his HP for validation of the vaccination records.



User journey 8:

Patient introduces his vaccination data and HP validates the data

Patient manually introduces his vaccination data record on his app. And asks his HP to validate the data in his vaccination record.



2.2. HP user journey

Neal Wilson, 40



Pharmacist (80%)
Married, 2 kids (8 and 11)

Bio: Managing director, tries to reconcile job and family, wife also works 50%, lives outside the city

Life Style: loves to travel and spend time with the family. He likes to go biking and read books. He supports the digitalization and tries not to lose touch (needs support)

Needs: more hours in the day, good processes, less administrative work, rapid access to services, quality and advice

Pains: organizes the household and the pharmacy, a lot of stress, too less time

Typical user journey

Reference to chapter 2.1: User Journey 1

Initial situation: The customer is already registered on the platform.

Appointment

The patient makes an appointment by phone/online booking for the yearly influenza vaccination. He asks the client if she has a MIDATA account. The patient answers yes. The pharmacist asks the patient to check and activate the required consent in his MIDATA profile to enable him. The patient logs on to MIDATA and notes that he has not yet given the pharmacist a consent. The patient grants access to the pharmacist via MIDATA consent management and gives the corresponding consent (see [2.9.2. HP onboarding and authentication](#)). The pharmacist opens the primary system and Documedis. He is logged in directly via HIN. The pharmacist searches for the patient's MIDATA account in Documedis and finds him due to the granted access rights by the patient via patient app/MIDATA.

Identification & Overview	<i>The customer appears for the appointment. The pharmacist checks the identity, opens the primary system and Documedis. In Documedis he can find the patient and view all previous vaccinations via an overview button (interface MIDATA). If the patient did not have an account yet, the HP could create one with him/her. See user journey 2 in chapter 2.1.</i>
Preparation	<i>The pharmacist fills out the questionnaire in Documedis. Based on the questions, the pharmacist collects the medical history and the necessary information before giving the vaccination (This information is for the personal records of the HP). The collected medical history is part of the electronic health record and saved in the primary system by the HP app.</i>
Vaccine	<i>The HP gives the vaccine to the client.</i>
Documentation	<i>In Documedis, the pharmacist enters the details of the vaccine (Immunization Administration). When he has finished, he confirms the information entered. He then saves it in the MIDATA (and optionally in his primary system) account and in his primary system.</i>
Billing	<i>The pharmacist does the billing as usual in the primary system</i>

David Smith, 56



Bio: *successful career, live outside the city in a nice residential area*

Life Style: *enjoys spending his free time with his wife playing golf or on the ski slopes. He also meets his two brothers once a week for dinner. Accepts digitalization but finds it difficult to adapt his usual processes.*

Family doctor (100%)
Married, no children

Needs: good processes, less administrative work, rapid access to services, quality, advice and regular support

Pains: not enough time for patients, stressful situations, not much time to recover

Typical user journey

Reference to chapter 2.1: User Journey 1a, 1b, 2, 3

Initial situation: Client does not yet have a digital vaccination booklet and would like to make a trip to Africa.

Telephone agreement

Client calls the doctor to ask which vaccinations she needs for a trip to Africa. The doctor asks if she has a digital vaccination booklet. The client answers no. The doctor asks her to create one, to enter the existing vaccinations, to give him the authorization and makes an appointment. To do so, the HP gives by phone the code to the Patient, so that the patient can enter the code of the HP in the patient app (see patient journeys in Patient Journey 1a, 1b, 2, 3).

Confirmation of existing vaccinations

At the appointment, the doctor opens the primary system and Documedis. With the HIN login, the HP can login into MIDATA. The doctor searches for the patient's MIDATA account in a field in Documedis. This is due to the granted access rights by the patient via MIDATA. Since the client has authorized it, the doctor now has access to her data. He compares the information in the Documedis system with the information in the physical vaccination book. He then confirms the information that the patient has provided independently.

Vaccination recommendation

The doctor receives the new vaccination recommendations by pressing the regarding button in Documedis. He can indicate that the client wants to travel to Africa and then receives the recommendations for the additional immunization.

Preparation

The doctor fills out the questionnaire in Documedis. Based on the questions, the doctor collects the medical history (based on the questionnaire in Documedis) and the necessary information before giving the vaccination (This information is for the

personal records of the HP). The collected medical history is part of the electronic health record and saved in the primary system by the HP App.

Vaccine

The HP gives the vaccine to the client.

Documentation

In Documedis the doctor enters the details of the immunization vaccination. When he has finished, he confirms the information entered. He then saves it in the Patient MIDATA account and in his primary system.

Billing & appointment

The client makes the appointments for the further vaccinations and the corresponding billing is carried out by the doctor in the primary system.

Nicole Miller, 31



Hospital physician (100%)
Boyfriend, just moved in with

Bio: *at the beginning of her career, her boyfriend is also a doctor, they live in the city*

Life Style: *plays tennis and goes jogging regularly. Enjoys free time with friends or colleagues drinking coffee or having brunch. Does not like to plan ahead, often forgets appointments and is not well organized. Would like to have three children. She has grown up with digitalization. She cannot imagine everyday life without a smartphone.*

Needs: *clear information, simple overview, rapid access to services, access to all data online*

Pains: *too much paper, no overview, often forgets something*

Typical user journey

Reference to chapter 2.1: User Journey 5, 7, 7b, 8

Initial situation: Doctor and patient are registered

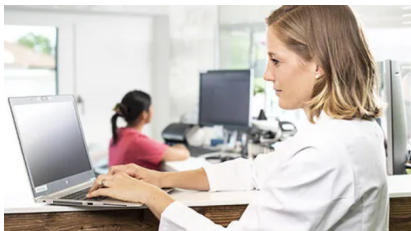
Doctor starts new job at the hospital

The doctor starts her new job at the hospital and receives a corresponding HIN account. One of

her tasks in the department is to validate vaccinations.

Notification	<i>The doctor gets a call from a patient who is asking for validation of a vaccination.</i>
Access	<i>The doctor opens Documedis via the primary system and searches for the corresponding patient. The patient gives the doctor access to his dossier.</i>
Review and correction	<i>The doctor checks the information and the uploaded proof of vaccination (photo or scan of the vaccination booklet). She notices that the patient entered the wrong year when entering the date. She corrects the date of the vaccination and then confirms it.</i>
Comment	-

Diana Taylor, 36



Hospital physician (100%)
Lives alone, no children

Bio: Experienced doctor with ambitions, lives in the city right next to the hospital

Life Style: plays in a local soccer club in her spare time and is a soccer coach herself

Needs: Investment in new medical technology, more physicians assistants in the department for support

Pains: too little time for her hobby as a footballer, Staff shortage leads to more work

Typical user journey:

Reference to chapter 2.1: User Journey 7

Initial situations: the patient provides to the HP his XML file of the meineimpfungen.ch dossier and asks his HP to update his vaccination record with the given data.

Appointment

The patient makes an appointment by phone or online to book an appointment for the seasonal influenza vaccination. The patient is a digitalization enthusiast and brings his old meineimpfungen.ch dataset by XML on a USB stick which he got by mail a few weeks ago. The patient asks the physician if he can import his data into his already existing MIDATA account. The physician answers yes.

Access

After the patient checked and activated the required consent in his MIDATA profile to enable the HP, the HP can begin to transfer the old meineimpfungen.ch patient data.

Import of the XML dataset

The HP imports the dataset through his primary system and therefore the HP app, which is already connected with the primary system.

Validation

The HP validates the imported data by accessing the patients vaccination booklet using the HP app.

2.3. Data entry by patient

Prerequisite

The patient has created a MIDATA patient account, either by self-registering via the web-app or by completing a registration process initiated by an HP (see [2.8. Patient account lifecycle management](#)). Patient's mandatory data, including email, mobile and date of birth are stored in his personal MIDATA account.

By logging in on the patient app, the patient can introduce recent or old vaccination data. Old vaccination information can be automatically imported from an XML file generated by the previous vaccination systems or be added manually via an entry form. Both options ensure that the data entered by a patient is always structured. A scanned copy or a photo of a proof of vaccination (i.e. old paper vaccination booklet) can also be uploaded.

The patient can change, delete or add vaccination info at any time.

However, data entered and/or validated by an HP cannot be edited by the patient without the invalidation of the immunization record. In this case the patient will be informed by the web-app before confirming to proceed with the editing. Only correctly introduced immunization data are processed by the CDS system.

The patient can then choose to cancel his action or to move forward being aware of the consequences, in which case he might want to ask an HP to validate the changes made.

To do so, the patient starts by introducing his immunization documentation and can "optionally" upload a PDF or a photo of the document as proof of the vaccination which can accelerate HP validation process. This process can be repeated several times.

The patient chooses the menu "Introduce my vaccination data" on the patient app. The patient can then introduce the vaccination and information and eventually upload the corresponding PDF or photo of the document as an option. The information to be introduced are basically the following:

- Type of vaccination: mandatory field. Drop down list with vaccines list and value "Other" with possibility to enter a text manually if not available in the list. The specific vaccination immunization data will be checked by the HP during the validation process
- Date of vaccination: mandatory field
- Dose: optional
- By whom: optional, text field
- Reason for vaccination: drop down list with values: Sickness, Prevention, Travel, etc. (optional)
- Batch number (optional)
- Where: optional text field

- Introduced by: "Patient" - automatically filled and mandatory. If filled by HP, the HP name will be automatically filled.

The patient can fill in several immunization documentation and add a PDF or a photo of the document per record.

The data is then available in the vaccination record of the patient as vaccination data to be validated by HP. The HP may validate these data on the patient's request, requiring he has been granted authorisation by the patient.

This data can also be accessed and read by HP if they have granted access as part of the vaccination record. An HP can modify the data and complete with new data entry if needed.

The structured data can be changed afterwards if needed by an HP if any errors are found.

2.4. Data entry by HP

The HP opens the primary system and Documedis or he may directly open Documedis without the primary system. In Documedis, he fills out the appropriate questionnaire for the vaccine, consisting of questions about the patient's medical history:

- Allergies (1)
- Pregnancy (1)
- Regular medical checkup (2)
- Underlying diseases (2)
- Consent of the patient (2)
- Past vaccinations for this disease (3)
- Immunodeficiency (3)
- Blood risk (3)
- Taking medications (3)
- Current health status of the patient (3)
- Previous vaccines (3)
- Side effects of previous vaccines (3)
- Fainting or nausea from previous vaccines (3)

Some of this information might of course be fetched from the primary system, avoiding manual data entry.

As these information have different impact on the CDS decision, they are classified in three different categories:

- Category 1: can impact the CDS decision
- Category 2: might help and have an impact in the decision making of applying the immunization proposition
- Category 3: the relevance of this information to the CDS is not yet fully established, HCI Solutions is currently working on the detailed specification.

In addition, he gives the exact details of the vaccine:

- Name of the vaccine
- Lot number
- Vaccination date

Finally, the HP can (there is no documentation duty) save all information into his primary system and enter the vaccination into the patient's vaccination record (the dataset specification of immunization administration is to be found in [chapter 3.2.2](#)). When the HP records the vaccine via HP app and stores it in the patient's vaccination record, the vaccine is automatically considered validated and confirmed.

The questions may vary depending on the vaccine. Most of the questions are only relevant for the documentation of the HP. When the HP wants to save the vaccine in

the patient's vaccination record he will see (displayed as a popup in his HP app) an overview of the data which will be stored. Accordingly, not all data will be transmitted to MIDATA. The data which are relevant for the vaccination record are described in the table hereafter.

#	Field Name	Type	Description
1	patient_id	String	ID of the patient in MIDATA
2	vacc_name	String	Name of the vaccine
3	disease	String	Disease against which the vaccine is administered
4	vacc_lot_number	String	Lot number of the used vaccine
5	vacc_id	String	Vaccine ID (GTIN)
6	vacc_date	Date	Date of vaccination
7	vacc_count	Integer	Vaccination count; denotes the number of vaccinations received for this vaccine: 1 = first vaccination 2 = second vaccination ... = nth vaccination
8	responsible_HP	String	GLN of the responsible health professional
9	reporting_unit_location_ctn	String	Canton in which the vaccination was administered: XX canton code or FL or AA (for Swiss Army)
10	reporting_unit_id	String	Reporting unit ID (e.g. 1234abcd). Unique identifier issued upon registration of the technical interface

11	reporting_unit_location_id	String	Reporting unit location ID. Shall allow for tracking active vaccination locations per canton and reporting units. Unique within every reporting unit. Is to be defined/specified by the corresponding reporting unit.
12	reporting_unit_location_type	Integer	Reporting unit location type (code): 1 = vaccination centre 2 = nursing home 3 = medical practice 4 = pharmacy 5 = hospital 6 = army 99 = other
13	route_of_administration	String	Path by which a vaccine is taken into the body
14	next_dose	Integer	Tells whether another dose is needed: 0 = no 1 = yes
15	date_next_dose	Date	Date of next vaccination. Shall be used for the reminder to the patient.

2.5. Patient onboarding

Here below is a list of minimal demographic data requested for the creation of a new MIDATA patient account (specific data requirements can vary over time depending on use cases and regulation):

- last name
- first name
- date of birth
- email address

For the patient onboarding we consider two main use cases based on who is performing the registration of the patient.

2.5.1. Patient registration by HP

The HP, connected to Documedis, searches for a specific patient (search criteria described in [chapter 2.10](#)), the search request is forwarded to the MIDATA backend. In case MIDATA returns no results to the search query, there are, in line with the implemented confidentiality principles (see chapter [7. Security by design](#)), two possibilities: 1) the patient doesn't have a MIDATA patient account, or 2) the patient has a MIDATA patient account, but a consent between the patient and the HP is not present.

In case condition 2) is true, the HP can directly request the patient to scan his personal HP QR code via the patient app to trigger a consent request (see [5.3.3.3. Creating the consent](#)).

Alternatively, in case the patient is not yet a MIDATA account holder, the HP can initiate a "proposed consent" procedure directly via Documedis, providing the patient's email and demographics data; this procedure will trigger the creation of a new MIDATA account and the registration of a consent between the registering HP and the patient itself.

When receiving the proposed consent, MIDATA verifies the pre-existence of a patient account associated with the email provided within the proposed consent received via Documedis.

1) If a patient account is found in MIDATA, the proposed consent is linked to the identified account, and an email is sent out to the account holder to confirm the consent request.

2) Alternatively, a registration procedure is initiated if the email address provided with the proposed consent is not already linked to an existing MIDATA account. An email containing a time-expiring and encrypted token is sent out to the registering patient. The encrypted token holds information like email, demographic data, and consent-id, and it is provided to the user in the form of a URL. By following the link, the patient is forwarded to a pre-populated registration web-form. All the fields can be edited before confirmation, including the email address (in this particular case a new verification email will need to be sent out to the patient to confirm the provided address).

The new user will also be requested to choose a personal password – which will be used to encrypt his personal data stored in the MIDATA account (see [7.7. Data encryption](#)) – and configure a 2FA authentication mean (e.g., m-TAN).

At this stage, if already in possession of a MIDATA account (associated with a different email address), the patient can directly log-in to MIDATA with his credentials, aborting the registration of the new account.

Either way, after completing the registration, or log-in with existing credentials, the patient is requested to confirm the acceptance of the specific terms of use and privacy policies and consent to authorize the registering HP to access his MIDATA account data.

To enhance the security of the proposed solution and minimize the risk that unauthorized individuals might gain access to the patient's demographic data, in addition to the already mentioned encryption system, the invitation link is provided with an auto expiry time-based mechanism.

This solution will ensure that:

- If the patient does nothing and ignores the received registration email, no personal information is stored on the MIDATA platform without the user's authorization (the HP provided data is only contained within the encrypted invite link). Moreover, if the invitation link is intercepted and exploited by an unauthorized third party, the short expiry date will ensure that the link won't be usable at a later stage, as the server will only decrypt the token if this has not expired.
- If an unauthorized user intercepts the link after the patient has already registered his account, MIDATA server recognizes that the link has already been used and promptly denies the decryption of the link. This ensures that unauthorized users cannot access any patient's demographic data.
- If an account already exists when the HP triggers the patient's registration, the MIDATA platform generates an email for the patient containing an encrypted link providing no personal demographics data but only the authorization request from the HP.

2.5.2. Patient registration via patient app

When accessing the patient app for the first time, the patient is requested to login with his personal MIDATA credentials or, in alternative, to proceed to the registration of a new MIDATA account (see [2.8. Patient account lifecycle management](#)).

New MIDATA user

By choosing to register a new account, the patient is redirected to a MIDATA miniportal. The miniportal presents the mandatory and optional registration fields that the patient is requested to fill in. The new user will also be requested to choose a personal password – which will be used to encrypt his personal data stored in the MIDATA account (see [7.7. Data encryption](#)) – and configure a 2FA authentication

mean (e.g., m-TAN). The registration proceeds with the invitation to the patient to read and accept the MIDATA *General Terms and Conditions* and *Privacy Policy* of the MIDATA platform as well as the terms specific for the patient app (see chapter [6. Legal](#)).

Existing MIDATA user

In this case, the patient already possesses a MIDATA account, previously created in the context of other projects or apps (i.e. AllyScience, CoronaScience, etc.). By entering his personal credential, the user is redirected to the review and acceptance of the terms specific for the patient app. The page will also request the review and acceptance of the MIDATA terms, only in case any modifications have been made to the text since the last patient's acceptance.

2.6. Data validation by HP

Data directly entered by HP is automatically validated.

Data entered by the patient, either manually or via the upload of an XML file, can be validated by an HP. The patient app provides a means to scan and store documents to be used as "proof of vaccination" (i.e. PDF, paper vaccination booklets). Those files can be accessed and reviewed by the HP during the validation process.

Once an immunization documentation or a Vaccination Record has been validated by a health professional and a second HP can edit and re-validate existing data.

The technical implementation of the validation procedure is presented in the architecture chapter (see [5.4.3. Validate existing data record](#)).

In order to have the HP validate the vaccination, a new functionality must be made available in Documedis (to be built). Documedis retrieves the data to be validated via MIDATA. The HP can display the information and then confirm or reject it. In both cases, the patient receives a notification. Detailed concept to be defined.

2.7. Notification by CDS

As the MVP does not envisage a direct connection/interface between the patient web app and the CDS, the notifications to the patient do not come from the CDS. The patient app should send push notifications to the patient when a vaccination should be refreshed. The notification could read: "It has been 5 years since your last TBE (FSME) vaccination. Please contact your doctor or pharmacist".

If multiple vaccinations are needed or if the vaccination is to be repeated annually, the HP can enter a reminder date for the next vaccination when the vaccination is recorded. On this date, the patient will receive a notification from the patient app and can then make an appointment for the vaccination.

The user of the patient app has the option to deactivate notifications in the settings.

2.8. Patient account lifecycle management

2.8.1. Account creation


The patient has to register (“Sign Up”) to MIDATA when he uses the patient app for the first time, unless he already has a MIDATA account. On registration, the patient has to enter personal contact information and demographic data and accept the *MIDATA General Term and Conditions* and the *MIDATA Privacy Policy*.

After the registration, or after the first login in case he already had an account, the patient must accept the terms of use of the patient app.

Once the registration is completed, the patient may use the patient app.


When connected to MIDATA, the patient might logout at any time. If he does so, he will have to relogin the next time he wants to access his data.


Sign Up



Please fill in the information below, fields marked with an asterisk (*) are mandatory. The password must be at least 8 characters long and contain one letter and one digit.

E-Mail*


Password* 


Repeat Password* 


Account Protection Increase the protection of my data with an additional security level. Warning: if I forget my password, it may take a few days until I can reset it.

First Name*

Surname*

Gender* 

Preferred Language* 

Country* 

Terms I accept the [General Terms and Conditions](#) and the [Privacy Policy](#)

2.8.2. Account ID / email change

The “Edit Profile” menu of the MIDATA portal offers patients the option to edit all their personal contact information and demographic data provided during registration.

In case the patient wants to change his email address, a validation process is initiated by sending a challenge code to the newly provided email address. Once the validation is completed successfully the account id of the user is updated with the new email address.

2.8.3. Password change

In the “Edit Profile” menu, the MIDATA portal provides password and 2FA change option for account holders correctly authenticated. In case of password loss, the portal also offers a password recovery procedure.

In case the patient requests to change his 2FA telephone number, a validation process is initiated by sending an SMS challenge to the provided phone number.

2.8.4. Data export

In line with the General Data Protection Regulation directives, a patient can decide to export all of his data records collected within MIDATA.

The function is available for all the MIDATA account holders via the MIDATA portal.

Data can be exported in their original format (JSON/FHIR).

2.8.5. Data deletion

A patient can use the function provided by the MIDATA portal to selectively delete specific data records.

When the patient chooses this function, the following steps are executed (these operations cannot be reverted):

- The patient can select which type of data must be deleted by choosing the specific resource type, with different granularity options (i.e. all immunization records) or by deleting all data produced by a specific application.
- The selected data entries are deleted.

These operations are recorded in the audit logs.

Logs are kept for a period of minimum 10 years.

2.8.6. Quit vaccination booklet ecosystem

A patient can use the functions provided by the MIDATA portal to cancel all consents with HPs that have been created during the use of the vaccination booklet

ecosystem. The vaccination data and demographics data shared by these consents will no longer be accessible by the HPs.

The data added to the patients account will remain as is unless the patient also deletes the data (see [2.8.5. Data deletion](#)) or his account (see [2.8.7. MIDATA patient account deletion](#)).

A patient can revoke the access of the patient app to his MIDATA account.

A patient can rejoin the vaccination booklet ecosystem by logging in again using the patient app and reaccepting the terms and conditions of the patient app. New consents for HP access may be created.

2.8.7. MIDATA patient account deletion

A patient can use the account deletion function from within the patient app or by logging in the MIDATA portal.

When the patient chooses this function, the following steps are executed (these operations cannot be reverted):

- All data are deleted
- All consent and associated keys are deleted
- All demographics information are deleted
- All login credentials are deleted
- All personal configuration data is deleted

These operations are recorded in the audit logs. Logs are kept for a period of minimum 10 years.

2.9. HP account lifecycle management

2.9.1. HP identity verification

As described in [4.1. HP ID and login](#) a correct and secure identification of health professionals, as well as the validation of their specific role and license to operate, are mandatory requirements to ensure the security and reliability of the system and to guarantee the confidentiality of sensitive data.

For this reason, the identification and management of the digital identities of the health professionals relies on the Health Info Net AG (HIN) network, leading provider of health professional digital identities in Switzerland.

2.9.2. HP onboarding and authentication

Given that a HP has a HIN eID and access to Documedis, the HP will access the vaccination portal via Documedis and authenticate on the HIN login page. In the background, the system will check if the HP has a MIDATA HP account, create one if not

and authenticate on MIDATA using the authentication token provided by HIN (HIN SAML assertion).

On the first access to MIDATA, the HP will have to accept MIDATA's *General Terms and Conditions* and *Privacy Policy* for health professionals.

2.9.3 MIDATA HP login

A HP having been boarded via Documedis will be able to log in the MIDATA portal using his HIN login. The only purpose of logging into the MIDATA portal is for the HP to be able to delete his MIDATA HP account.

2.9.4. MIDATA HP account editing

HP accounts will be created in MIDATA based on the trusted information obtained from HIN (see [2.9.2. HP onboarding and authentication](#)). Thus, they will not be editable in the MIDATA portal. MIDATA will update HP's data (from the HIN SAML assertion) on every connection of the HP to MIDATA.

2.9.5. MIDATA HP account deletion

HPs can use the account deletion function in the MIDATA portal. Like for patients (see [2.8.7. MIDATA patient account deletion](#)), the following steps are executed (these operations cannot be reverted):

- All data are deleted
- All consent and associated keys are deleted
- All demographics information are deleted
- All login credentials are deleted
- All personal configuration data is deleted

These operations are recorded in the audit logs. Logs are kept for a period of minimum 10 years.

If, after having deleted his account, an HP accesses MIDATA again using Documedis to consult or store patients' vaccination data, then a new MIDATA account will be created as described in 2.9.2. HP onboarding and authentication.

2.9.6. Generation of HP personal QR code/personal code

A HP must be able to generate a QR code and personal code in Documedis, that uniquely identifies him and that he might present to a patient for getting granted access to the patient's data (see [5.3.3 Authorize HP \(Consent\)](#)).

2.10. Search/authorize/linking patient-HP

General principles following the security and confidentiality requirements, see chapter [7. Security by design](#):

1. HPs can only look up for patients for which they have already received a consent
2. Patients can add and withdraw consents from the patient app when connected with their MIDATA account
3. The process of a patient authorizing an HP is simplified by the use of a HP personal QR code that must be scanned by the patient via the app or by the use of a HP personal number (univoquely provided to the HP) that must be manually entered by the patient in the app.

2.10.1. Patient use case

Pre-condition

In order to be able to consent and authorize an HP, the patient needs to own a MIDATA patient account and be connected to the patient app.

List relations

The patient is able to list all the consented health professionals who can already view and edit his vaccination information.

Add relation

We can imagine that a HP can contact the patient, formally asking to be granted access to his vaccination record. To simplify the authorization procedure and to minimize the likelihood that authorizations are provided to wrong HPs (i.e. homonymous HPs), the patient app provides the functionality to scan a QR code (provided by the HP) or to enter a personal code of the HP (also provided by the HP) that uniquely identifies the HP (see [5.3.3. Authorize HP](#)). After scanning the QR code or entering the HP personal code, the full name, GLN number, organization where the HP is active are displayed to the patient.

Remove relation

When a patient consults the list of his relationships, he is able to withdraw relationships no longer requested from the same patient app screen. The HP is not notified of the change.

2.10.2. HP use case

Pre-condition

The health professional is connected to the Documedis system and has a valid MIDATA HP account connected to a personal HIN eID (see [2.9.2. HP onboarding and authentication](#)).

Existing patient in MIDATA

In this case, the patient owns a valid patient account in MIDATA and he has authenticated himself via the patient app.

Via Documedis the HP can request the generation of his QR code and personal code. These codes are then provided to the patient that, by scanning the QR code, or manually entering the personal code, via the patient app, consents to the HP. Before consenting, the patient is informed of which data will be shared with which HP (nominally the demographics data and the vaccination administrations). The operation is recorded in the audit logs.

New patient in MIDATA

In this case the patient has not yet registered his account on MIDATA.

The HP can propose the registration of a new consent in MIDATA. This procedure triggers the registration of a new patient account, as described in [2.5.1. Patient registration by HP](#). The registration terminates with the patient reviewing and accepting the consent terms (which data are shared with which HP). In case the patient decides to deny the consent to the HP after registration of a MIDATA account, the registration process is not rolled back.

List relationships (patients)

Documedis application offers authenticated HPs the function to search and retrieve patient data. Due to the confidentiality constraints of the vaccination booklet solution proposed here, the search only returns registered patients for which a consent already exists.

Standard search criteria include any combination of last name, first name, date of birth, email address.

3. Data

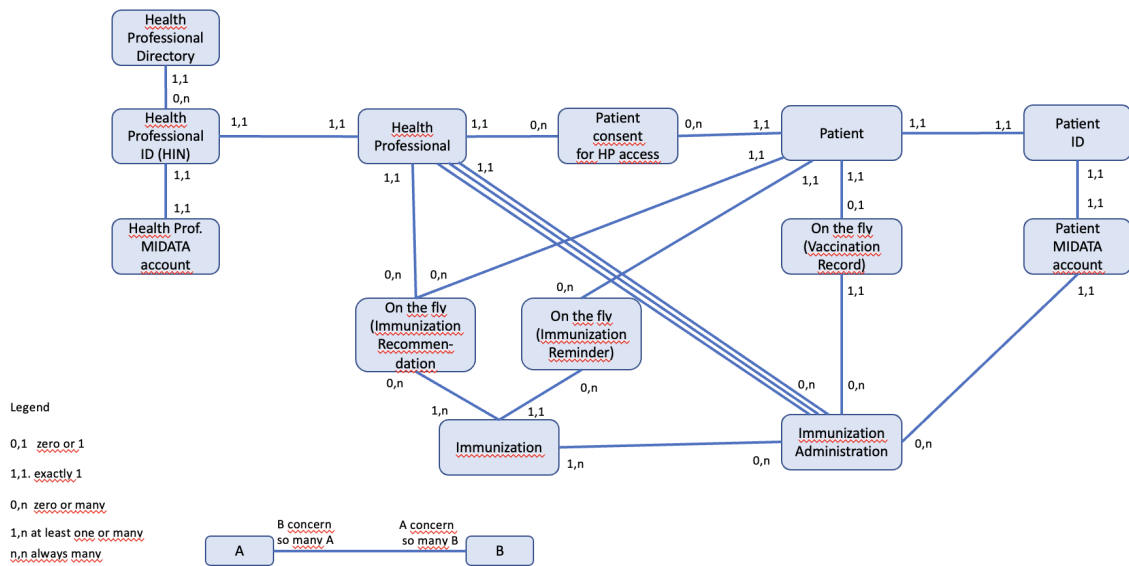
3.1. Data model

3.1.1. Entities

English	Remark	FHIR Format (see 3.2 for url references)
Patient	The patient getting the vaccine	Patient
Immunization administration	Data of an application of a vaccine to a patient for immunization reasons	Immunization
Vaccination record	Generated on the fly. In minimum the chapter with the known and applied immunizations	Composition
Vaccine	Vaccine product administered	Immunization.vaccine Code
Health Professional	The health professional administering the vaccine. A HP is accredited automatically by MIDATA based on his HIN eID	Practitioner
(MIDATA) Patient ID	Unique identifier of a patient	Patient.id
Health Professional ID	Unique identifier of a health professional (HIN eID)	Practitioner.id
Immunization recommendation	Generated on the fly by CDSS Module Immunization Recommendation Response containing all immunization recommendations which can be made based on the data delivered by the immunization recommendation request	Immunization Recommendation
Immunization reminder	Generated on the fly	N/A
HP MIDATA account	MIDATA account of a HP	N/A
Patient MIDATA account	MIDATA account of a patient	N/A
PDF file containing scans of paper booklet		Attachment

See [10. Glossary](#) for definition of terms.

The following diagram represents the data entity model. The content of each entity is described in [chapter 3.2](#), using the FHIR semantic.



Schema 3: Entity relationship model for the vaccination data ecosystem (according to https://en.wikipedia.org/wiki/Entity%E2%80%93relationship_model and UML representation).

The three relations between health professionals and immunization are:

- a) immunization administered by,
- b) immunization administration documented by,
- c) immunization administration documentation validated by.

They all have the same cardinality, but represent different roles and transactions.

Hypotheses to keep the solution simple and realizable within a short term:

- Patient consent is to single individuals (health professionals) and not to groups.
- Vaccination records include only immunization data and not allergies or diagnostics.
- Patient delegation would be treated only in later releases.

3.2. FHIR format

MIDATA provides a FHIR based API and stores all patient data in native FHIR format. FHIR stands for *Fast Healthcare Interoperability Resources* and is the newest standard for medical data exchange created by HL7. The actual version is FHIR Release 4 (<http://hl7.org/fhir/>).

The Swiss national Electronic Patient Record (EPR) also recently adopted the FHIR format as standard exchange format, replacing the initially selected CDA format (<https://www.patientrecord.ch/en>). To improve interoperability, national FHIR implementation guides are being specified by workgroups in collaboration with eHealth Suisse and HL7 Switzerland. They are documented on <https://fhir.ch>.

3.2.1. CH VACD

The implementation guide concerning vaccination is called CH VACD, “Implementation Guide for the exchange of vaccination and immunization information in Switzerland”, and can be found at <http://build.fhir.org/ig/hl7ch/ch-vacd/index.html>. The normative CI Build of CH VACD is currently under review before its final release.

CH VACD defines following documents:

Immunization Administration Document	Serves to document changes in the immunization status and contains information on applied immunizations and further relevant chapters as medical and exposition risks or serology results.
Vaccination Record Document	Compilation of all available immunization-related content and thus shows the patient's immunization status at a specific point in time
Immunization Recommendation Request Message	Contains all relevant data to be able to get an immunization recommendation from the clinical decision support system
Immunization Recommendation Response Message	Contains all immunization recommendations which can be made based on the data delivered by the immunization recommendation request

Here is for example the content of the Vaccination Record Document:



Schema 4: FHIR Bundle Vaccination Record document.

3.2.2. Relevant FHIR resources

All these documents are made up of one so-called *Bundle* resource of type *document* – a kind of envelope – containing a collection of further FHIR resources.

All resources used by the EPR implementation guides have been tailored to the Swiss specificities (this is called profiling). The relevant CH VACD FHIR resources are listed below:

Native resource	EPR profile	Link
Composition	CHCoreCompositionEPR	http://fhir.ch/ig/ch-core/StructureDefinition-ch-core-composition-epr.html
Patient	CHCorePatient	http://fhir.ch/ig/ch-core/StructureDefinition-ch-core-patient.html
Practitioner	CHCorePractitioner	http://fhir.ch/ig/ch-core/StructureDefinition-ch-core-practitioner.html
Organization	CHCoreOrganization	http://fhir.ch/ig/ch-core/StructureDefinition-ch-core-organization-epr.html
Immunization	CHVACDImmunization	http://build.fhir.org/ig/hl7ch/ch-vacd/StructureDefinition-ch-vacd-immunization.html
Provenance	-	http://hl7.org/fhir/R4/provenance.html
Condition	CHVACDCondition	http://build.fhir.org/ig/hl7ch/ch-vacd/StructureDefinition-ch-vacd-condition.html
AllergyIntolerance	CHVACDAllergyIntolerance	http://build.fhir.org/ig/hl7ch/ch-vacd/StructureDefinition-ch-vacd-allergyintolerances.html
Observation	CHVACDOtherRelevantObservations	http://build.fhir.org/ig/hl7ch/ch-vacd/StructureDefinition-ch-vacd-other-observations.html
MessageHeader	CHVACDRecommendationRequestMessageHeader	http://build.fhir.org/ig/hl7ch/ch-vacd/StructureDefinition-ch-vacd-recommendation-request-messageheader.html

4. Identification and authentication

4.1. HP ID and login

Which electronic ID should be applied?

Due to the advanced market development of the HIN identity, it is advantageous to use the HIN eID. In particular, the solutions already implemented at HCI (e.g. refdata login) have proven to be stable in the past, furthermore the HIN eID offers health professionals an already established and familiar login. In Documedis there is integrated the legal person for the COVID vaccination and the natural person for the certificate.

Integration of the HIN eID

The HIN eID can be connected via the HIN Access Control Service (ACS). Application providers can use ACS to connect their web applications and give the HIN community access to the services without an additional login. At the same time, the HIN ACS prevents unauthorized access by third parties ^[1].

This solution has already been implemented and is still used in various hospitals and pharmacies (like amavita) in Switzerland. Access to the secure HIN world requires an HIN membership.

Implementation in Documedis and MIDATA

The HIN login has already been implemented in Documedis. The HP logs into its primary system and a login via HIN is automatically performed. For registration, the login via the primary system (token-based) is sufficient. To be able to use MIDATA as well, the MIDATA OAuth endpoint can be used which will reuse the previously done HIN login to get a MIDATA session.

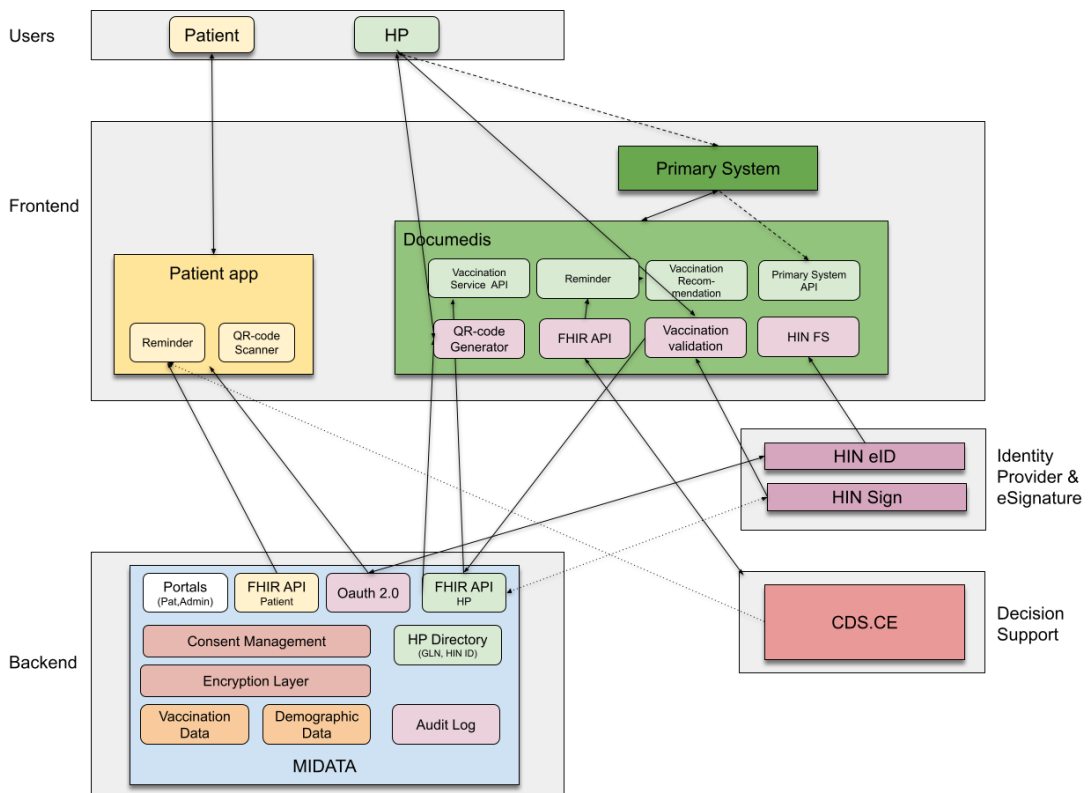
[1] <https://www.hin.ch/produkte/hin-access-control-service/>

5. Architecture & API

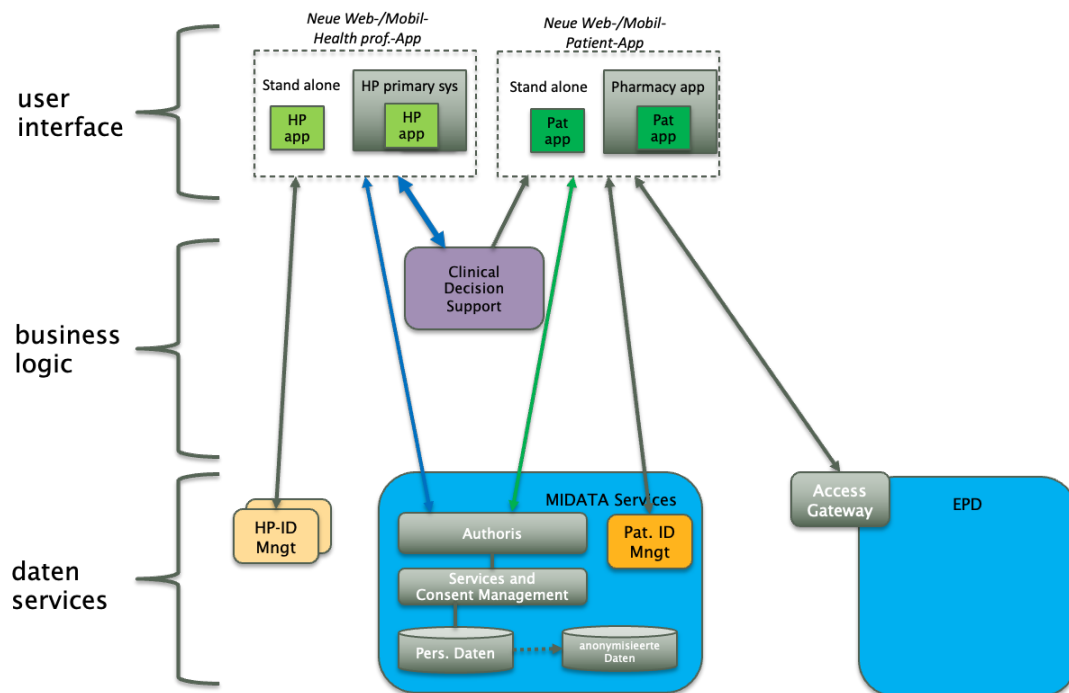
5.1. General architecture and components list

As this document is intended to describe an ecosystem-based solution, the proposed architecture follows the following principles:

1. Each component is a standalone system.
The complete set of functional and non-functional features, the details of their internal architecture, and their individual lifecycle processes are left out from this document as their application expands beyond the vaccination booklet scope.
2. To guarantee the interoperability of the current components and to prepare the future integration of additional third-party solutions, the proposed architecture relies on the availability of existing open APIs (application programming interfaces) as well as well-defined open standards wherever possible.



Schema 5: System architecture.



Schema 6: Software architecture.

Components overview

To provide the required functionalities, the Digital Vaccination Booklet solution consists of the following components:

Documedis

Documedis, which is operated by HCI Solutions AG, will be used as the HP app. It will provide to the HP the following functions: requesting patient's consent, search for patients, access to patient data, show all previous vaccinations of the patient, save a vaccination, receiving a vaccination recommendation, fill a questionnaire to record the medical history of the patient, access CDSS, creating a QR code and a personal code.

Documedis will not store any data. All data will either be stored in MIDATA or the primary system of the HP.

Documedis must be able to connect to the different HP primary systems, which is already part of the documedis architecture. The CDSS System will be part of Documedis, in a later step CDSS could be accessed via API through the patient app.

All functionalities regarding the operator of the Health Professional eID and directory are already implemented in Documedis and in use.

A QR code generator must be part of Documedis that may be scanned using the patient app to authorize a HP to access the patient's vaccination. The content data will be provided by MIDATA and triggered by the HP himself.

Patient app

The app provides to patients a user interface to upload, retrieve, display patient's data, setting and review authorizations and manage reminder notifications.

Provides the upload of XML files, PDF and pictures.

The app should be compatible with iOS and Android. The recommendation is to develop a Web App instead of native apps (Android and iOS) or Xamarin (common to both).

Depending on the final business model, but assuming that this functionality could also be branded, this means that Brand App (whether is an insurance, or an Amavita APP) should integrate APP. The easiest integration is if it is a "web app":

- It makes the release management of the APP independent on the brand apps.
- The integration cost in other brand is very low
- One development for Android and iOS
- Web app can also be access on PC (same interface) anywhere

Even though web apps might be more limited in some functionalities Like "notifications", there are workarounds to implement even if it might be more complex than Native Apps but makes the rest of cases much easier to handle.

MIDATA

In the context of the vaccination booklet use case, MIDATA provides:

- FHIR support for:
 - APIs for the management of patient accounts, for the storage and retrieval of patient's data and for the management of consents and authorizations
 - Data format of the personal data records. Personal data are stored in structured format using SNOMED and LOINC ontologies, with support for binary data and documents
- OAuth 2.0 services for the secure authentication of users. The service supports the integration with external Identity provider services as well as the integration with 2FA services (e.g., SMS)
- Web-portal for the registration of new patient accounts and review of the *General Terms and Conditions* and *Privacy policy*
- Storage of patient's personal data, including vaccination records, secured by a multi-layer encryption mechanism
- Management of dynamic consents, allowing patients to generate and manage data sharing policies with other users
- Web-portals for admin facilitating monitoring, configuration and operation management (i.e. change of terms and conditions).

Clinical Decision Support (CDS) Service

This component is provided as an integrated Software-as-a-Service (SaaS) solution, directly accessible via the Documedis web platform as CDSS module. It provides decision support capabilities helping Healthcare providers in providing better services to

their patients. The target classification is IIa. As a future idea (see [9.2 Not in MVP, optional features](#)) CDSS could be accessible by an API by the patient app.

HIN eID

HIN provides the enforcement of strong authentication and secure authorization of all HP taking part in the solution. The HIN eID is also used in the national Electronic Patient Record (EPR).

5.2. Support of FHIR API and concepts

This project supports the implementation of [Fast Healthcare Interoperability Resources \(FHIR\)](#) API as the main interoperability framework for the integration of the various components included in its main general architecture.

FHIR is a next generation standards framework created by HL7. FHIR is designed to enable the exchange of healthcare-related information. This includes clinical data as well as healthcare-related administrative, public health and research data. It is intended to be usable world-wide in a wide variety of contexts, including in-patient and ambulatory care. FHIR is seeing a fast rise in health IT, with broad adoption of the standard.

The MIDATA platform supports FHIR standards and concepts. The FHIR support layer is built on top of the core system. The core system itself stores data records in (encrypted) JSON format and is not FHIR dependent. It also provides some concepts for the management and sharing of the data.

Users

Each physical person that has access to the platform is a user. The concept of platform user is directly mapped to the FHIR resource type *“Person”*. In addition to *“Person”* for each user an additional *“Patient”* or *“Practitioner”* FHIR resource may be generated. There are different types of user accounts on the platform for the different roles a user may have regarding the platform.

Data Records

MIDATA is a document type store. Each single document is defined as a record and it may be represented by a single FHIR resource, a JSON document or a binary data.

Consents

The sharing of data records between users or applications is managed by consents. A consent always grants access to some FHIR resources of a single user to other entities. Consents may have a lifetime and may restrict access to data created during a limited period of time.

Using a consent the patient grants a HP read and write access to his immunization documentation. The patient must grant each HP separately. The consent grants access to the patient demographics, the immunizations and related documents, immunization recommendations.

See also following chapters:

- [2.5.1. Patient registration by HP](#)
- [2.10.2. HP use case](#)
- [5.3.3. Authorize HP \(Consent\)](#)

5.2.1. General FHIR resource interactions

5.2.1.1. Requests

MIDATA API must be able to consume and process the following requests

Interaction	Path	Request Verb	Request Content-Type	Body
read	/[type]/[id]	GET	N/A	N/A
update	/[type]/[id]	PUT	R	Resource
create	/[type]	POST	R	Resource
search	/[type]?	GET	N/A	N/A
(operation)	/[type]/\${name} /[type]/[id]/\${name}]	POST GET	R application/x-www-form-urlencoded	Parameters form data

N/A = not present, R = Required, O = Optional

The MIDATA API supports JSON and XML as format for the FHIR resources. Each request must have an “Accept” header with the expected response format. In addition each request with a body must have a “Content-Type” header with the used body format. The provided value must include the FHIR version to be used.

The following two formats are supported for FHIR resources:

```
application/fhir+json; fhirVersion=4.0
application/fhir+xml; fhirVersion=4.0
```

5.2.1.2. Responses

MIDATA API must produce the following responses:

Interaction	Response Content-Type	Body	Location	Content-Location	Versioning	Status Codes
read	R	R: Resource	N/A	R	ETag	200, 404, 410
update	R	R: Resource	N/A	R	ETag	200, 201, 400, 404 405, 409, 412, 422
create	R	R: Resource	R	R	ETag	201, 400, 404 405, 422
search	R	R: Bundle	N/A	N/A	N/A	200, 403
(operation)	R	R: Parameters /Resource	N/A	N/A	N/A	200, 400, 403, 404, 422

N/A = not present, R = Required, O = Optional

5.2.1.3. Response codes

MIDATA API must produce the following main [HTTP status codes](#):

HTTP Status Code	Description
200	OK
201	Created
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
405	Method Not Allowed
409	Conflict
410	Gone
412	Precondition Failed
415	Unsupported Media Type
422	Unprocessable Entity
500	Internal Server Error
501	Not Implemented

5.2.2. Common functionalities

5.2.2.1. Search patient

HPs can only search for patients with an active consent with the HP. The search will automatically be restricted to this set of patients. Any search parameters provided by FHIR 4.0.1 may be used to retrieve the *Patient* resources. Typical searches would be by name and birthdate or by email.

Retrieve patients by name and birthdate:

```
GET <baseurl>/fhir/Patient?family=Meyer&given=Sarah&birthdate=eq1979-06-30
```

Retrieve patients by email:

```
GET <baseurl>/fhir/Patient?email=sarah.meyer@example.com
```

The *Patient* resources contained in the result FHIR *Bundle* each have an “id” field with the internal patient ID. This id can be used for further queries.

5.2.2.2. Retrieve data

For data retrieval FHIR resources Immunization, Composition and ImmunizationRecommendation may be queried. As a HP may have access to the data of multiple patients each query must be restricted by patient.

List all Immunizations of a patient:

```
GET <baseurl>/fhir/Immunization?patient=5e28407893de8a4be3e184f7
```

5.2.2.3. Adding data

New resources may be added either one by one by using a POST request on the resource base URL or all at once by sending a transaction bundle to the FHIR base url.

If data is added by the HP the patient field in the new resources must be populated using a reference to the patient resource that must have been queried before.

If data is added by the patient itself the patient field may be left blank and will be automatically populated with the account holders id.

5.2.2.4. Updating data

In order to modify an already existing resource it must first be fetched from the server. The modified resource can then be transferred back using a PUT request.

```
PUT <baseurl>/fhir/<Resource>/<id>
```

The original field meta.versionId must be retained in the resource as read from MIDATA. If the field is missing the update will be rejected with a HTTP status 412 “Precondition

failed". If the field differs from the version stored in MIDATA the request will be rejected with HTTP status 409 "Conflict".

Each update will create a new version of the modified resource. The old version may still be retrieved using FHIR history operations.

5.2.2.5. Deleting data

MIDATA does not support the DELETE operation. If data was provided in error the status of the FHIR resource may be changed to "entered-in-error".

5.3. Patient app to MIDATA

5.3.1. Register new patient

The patient app does not do the patient registration itself using the API instead the patient registration is done during the OAuth 2 login of the app.

The minimal set of parameters for OAuth login is:

```
https://<baseurl>/authservice?  
  response_type=code&  
  client_id=<client_id>&  
  redirect_uri=<redirect_uri>
```

To simplify registration the patient app may provide the user's country and the app's language as additional parameters:

```
  country=ch&  
  lang=de
```

After registration or login the control is given back to the patient app (via the redirect URI).

The response from the token exchange looks like:

```
{  
  "state": "none",  
  "access_token": "QIBlyHIxRbEw78...SUq9B6TiIsJ1ut5cFg",  
  "token_type": "Bearer",  
  "scope": "user/*.*",  
  "expires_in": 21600,  
  "patient": "56ded6c179c7212042b29984",  
  "refresh_token": "puvnkwSokP...oRHTrvfp1LnF-A"  
}
```

5.3.2. Add new data record

At first a session needs to be established using OAuth2. The retrieved Bearer token needs to be included in the “Authorization” header of each request.

New resources may be added by providing a bundle with the new resources. The “patient” field in each Resource may be left empty and will automatically be populated with the app sessions patient id.

Practitioner resources should not be contained in patient provided data. Either no practitioner information should be present or practitioner is only referenced by name using only the “display” field in the FHIR practitioner reference.

Example request:

```
POST <baseurl>/fhir
```

5.3.3. Authorize HP (Consent)

Only the patient can authorize a HP to access his immunization data. This is done by creating a new consent on MIDATA. In order to be able to create a consent with the HP the patient app needs to know which HP to authorize. There are two possible ways to identify the HP.

- a) By scanning a QR code that has been printed by the HP
- b) By manually entering a unique practitioner code for that HP

5.3.3.1. QR code

The QR code is scanned using the patient app to authorize a HP to access the patients vaccination data and needs to contain this information:

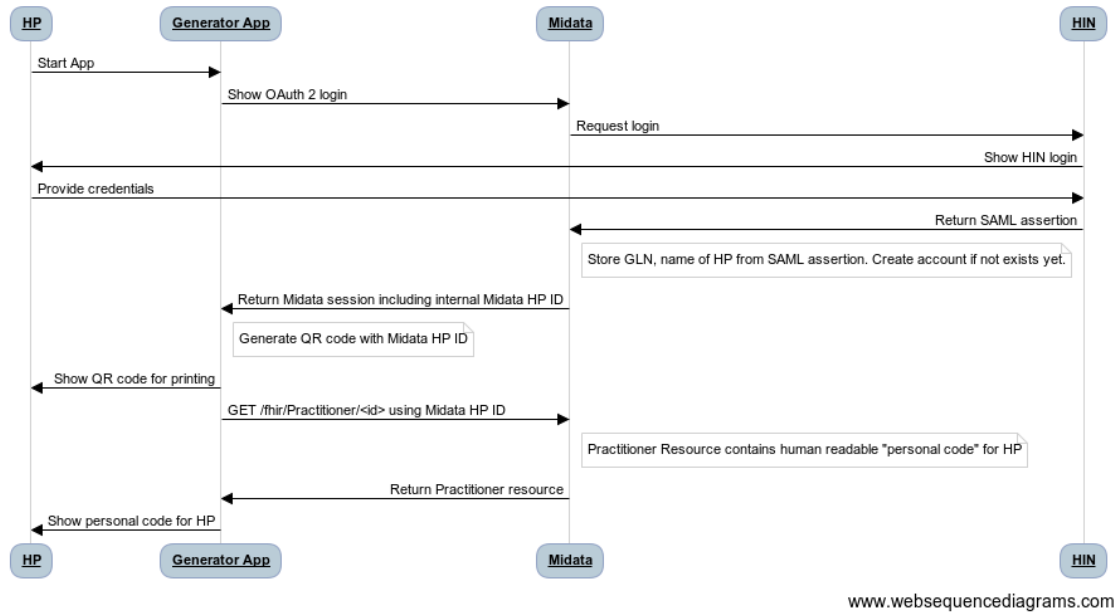
- The GLN of the HP that is returned by the MIDATA OAuth 2 log-in process.
- A fixed unique id for the vaccination use-case. The patient app should verify that the unique id is as expected.

The QR code is generated by Documedis that has no purpose beside uniquely identifying the HP. The request for a QR Code will be triggered by the HP and the request forwarded by Documedis to MIDATA. MIDATA then provides the content described above and Documedis generates the QR Code.

5.3.3.2. Personal code

The personal code is an alternative to the QR code if no code scanning is possible. (i.e. during a phone call). It should not be too long to be usable. A 10 digit personal code containing a checksum is generated by MIDATA during account creation. The QR code generating app may also be used to show his personal code to the HP.

For the generation of the QR code and personal code these steps need to be done:



Schema 7: Sequence diagram "Create QR and personal code".

5.3.3.3. Creating the consent

The patient app may authorize a HP by creating a new consent on MIDATA.

First the HPs QR code is scanned or the personal code of the HP is manually entered into the patient app.

If not already done the patient app must start a session with MIDATA.

Then a consent like this may be pushed to MIDATA.

```

POST <baseurl>/fhir/Consent
{
  "resourceType": "Consent",
  "status": "active",
  "category": [
    {
      "coding": [
        {
          "system": "http://midata.coop/codesystems/consent-category",
          "code": "default"
        }
      ]
    }
  ],
  "patient": {

```

```

    "reference": "Patient/56ded6c179c7212042b29984"
  },
  "dateTime": "2021-09-12T14:49:04+02:00",
  "policy": [
    {
      "uri": "http://hl7.org/fhir/ConsentPolicy/opt-in"
    }
  ],
  "policyRule" : {
    "coding" : [
      {
        "system" : "http://midata.coop/codesystems/policies",
        "code" : "vaccination-ecosystem"
      }
    ]
  },
  "provision": {
    "actor": [
      {
        "role": {
          "coding": [
            {
              "system": "http://hl7.org/fhir/v3/RoleCode",
              "code": "GRANTEE"
            }
          ]
        },
        "reference": {
          "reference": "Practitioner/5b178c4d79c7213e4ea992eb"
        }
      }
    ]
  }
}

```

The policy rule code is a fixed value.

The patient id may be taken from the OAuth login result.

The practitioner id may be taken from the QR code. If the personal code was used instead of the QR code the practitioner reference shall look like this:

```

"reference": {
  "identifier" : {
    "system" : "http://midata.coop/identifier/personal-code",
    "value" : "12345"
  }
}

```

Only the patient himself is allowed to add an active Consent to his account.

5.3.4. Send reminders to patients

MIDATA may be used as a storage for Immunization recommendations. These recommendations need to be generated by the external CDS system. The recommendations may be stored using a FHIR ImmunizationRecommendation resource.

The FHIR ImmunizationRecommendation resource is a point-in-time recommendation for future immunizations. New recommendations need to be generated after each immunization.

It is up to the patient app to retrieve the ImmunizationRecommendations and check that there is no Immunization resource which is newer than the newest set of recommendations.

The patient app manages internal push notifications based on the retrieved recommendations.

5.4. HP app to MIDATA

5.4.1. Register a new patient

The HP wants to establish a consent with the patient. First the HP will search for the patient on MIDATA using the name and birthdate. The patient will only be found if the HP already has an active consent with the patient.

If the patient has been found, the patient id can be used to search, add or modify patient data.

If the patient has not been found, the HP may provide the patient's email and demographic data to Documedis. Documedis creates a "proposed" *Consent* FHIR resource. The proposed consent contains a "contained" *Patient* resource as "grantor". The contained *Patient* resource contains email and demographic data. Documedis posts the proposed consent to MIDATA.

MIDATA checks if there is an account holder with the provided email address. If yes the consent is linked to this account and an email to confirm the consent is sent to the account holder.

If there is no account holder with the provided email address an invitation email is sent to the provided email address. An encrypted token is generated containing the email, demographic data, consent id and expiration date. A link containing the token is included in the email text.

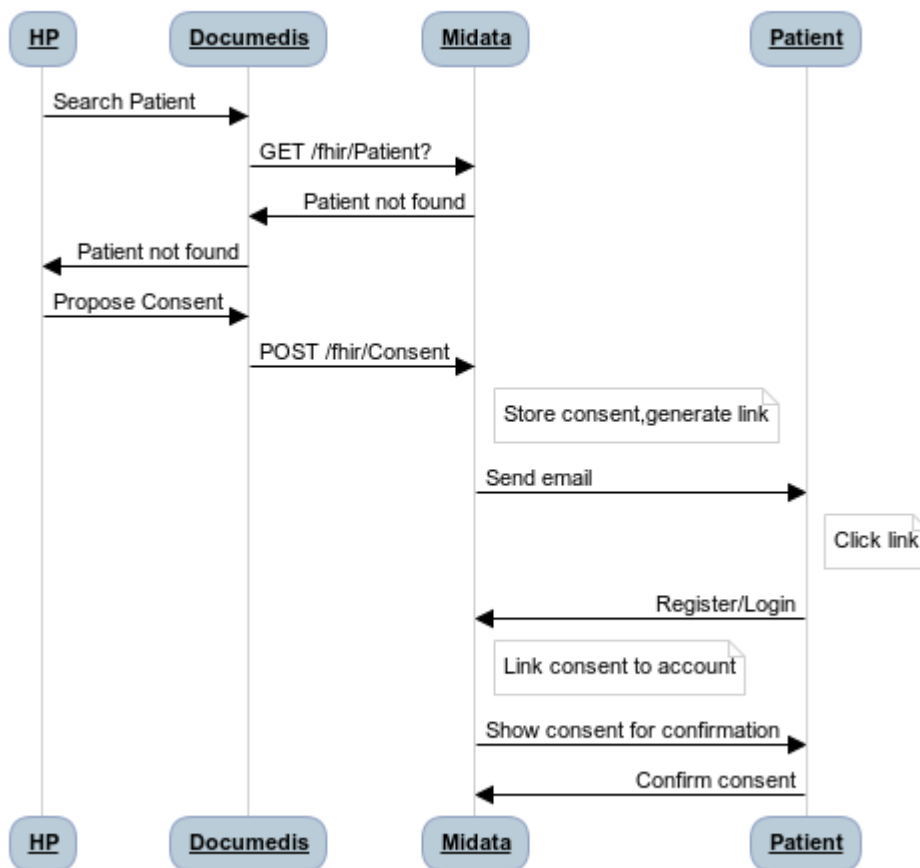
The user can click on the link. The encrypted token is decrypted by MIDATA if the expiration date has not passed and the consent is not linked to an MIDATA account yet.

The user may register an account with fields pre populated from the token or log in using his existing account with a different email address.

In case of a new registration the email address validation may be skipped if the account email matches the email used for the token. As the token has only been sent by email the user has proven ownership of the email account by clicking on the link. This is important as waiting for another email with confirmation would interrupt the process.

After registration / log-in the consent from the token is linked to the user account that logged in.

The consent to be confirmed is displayed in the browser and the account holder may click on accept or reject.



Schema 8: Sequence diagram “Register a new patient”.

The *Consent* resource that needs to be pushed to MIDATA to trigger the invitation process looks similar to the consent that is created by the patient app. The main difference is that the patient demographics are included. This is done by using a FHIR contained resource as target for the patient field. Also the consent status cannot be active as the patient still needs to confirm.

```

{
  "resourceType": "Consent",
  "contained" : [
    {
      "resourceType" : "Patient",
      "Id" : "p1",
      "name" : [ {
        "family" : "Meyer",
        "given" : ["Sarah"]
      }],
      "telecom" : [ {
        "system" : "email",
        "value" : "sarah.meyer@example.com"
      }],
      "gender" : "female",
      "birthDate" : "1979-06-30",
    }
  ],
  "status": "proposed",
  "category": [
    {
      "coding": [
        {
          "system": "http://midata.coop/codesystems/consent-category",
          "code": "default"
        }
      ]
    }
  ],
  "patient": {
    "reference": "#p1"
  },
  "dateTime": "2021-09-12T14:49:04+02:00",
  "policy": [
    {
      "uri": "http://hl7.org/fhir/ConsentPolicy/opt-in"
    }
  ],
  "policyRule" : {
    "coding" : [
      {
        "system" : "http://midata.coop/codesystems/policies",
        "code" : "vaccination-ecosystem"
      }
    ]
  },
  "provision": {
    "actor": [
      {
        "role": {
          "coding": [

```


Search for immunizations:

```
GET <baseurl>/fhir/Immunization?patient=<patientid>
```

Search for immunization documents:

```
GET  
/fhir/Composition?subject=<patientid>&type=http://snomed.info/sct  
/41000179103
```

Reconstruct document bundle for a composition returned by the previous search:

```
GET /fhir/Composition/<id>/$document
```

5.4.3. Validate existing data record

A vaccination record might be signed digitally in MIDATA by storing a FHIR resource *Provenance* containing the signature of the HP performing the validation with the vaccinate record (FHIR resource *Immunization*) as *target*.

5.5. HP authentication services

Health professionals who wish to access the digital immunization record data must authenticate themselves through strong authentication and their identity must be confirmed. For this reason, only HP who have been registered by HIN and have an appropriate status can log in.

Basics

When the HP calls Documedis from the primary system, he is automatically logged in with the HIN login with which he is logged in to the primary system. If he does not want to work with this login, he can log out and log in again manually. If he wants to use a service for which his current login is not authorized or for which an additional access authorisation is required, Documedis will redirect the HP to the HIN page (see procedure below). When Documedis is called up, it can also be checked whether a corresponding contract between the HP and HCI exists for his GLN (if necessary).

Necessary steps for the authentication of the HP and connection to MIDATA

1. HP must log in to Documedis:
 - a. Redirect to HIN
 - b. User enters password and confirms with second factor if necessary
 - c. User is authenticated
 - d. If no additional authorisation is necessary -> return to Documedis, otherwise see 2.

2. HP must allow Documedis access to 3rd application (MIDATA)
 - e. Documedis redirects to an OAuth 2 login page for HPs on MIDATA
 - f. MIDATA will create a SAML login request for HIN
 - g. If necessary, the user enters the password and/or second factor on the HIN login page.
 - h. User is authenticated, control is passed back to MIDATA.
 - i. MIDATA processes the SAML assertions and either creates a HP account for the provided GLN on MIDATA or logs in the existing HP account on MIDATA.
 - j. MIDATA returns an OAuth code back to Documedis which can be exchanged for a MIDATA session token.

3. As soon as HP is authenticated and has allowed access to the 3rd application, it returns to Documedis and the data can be transferred to MIDATA.

HCI has made this connection based on the HIN documentation “3.1.2 - Variante b): Übermittlung über Query Parameter”:

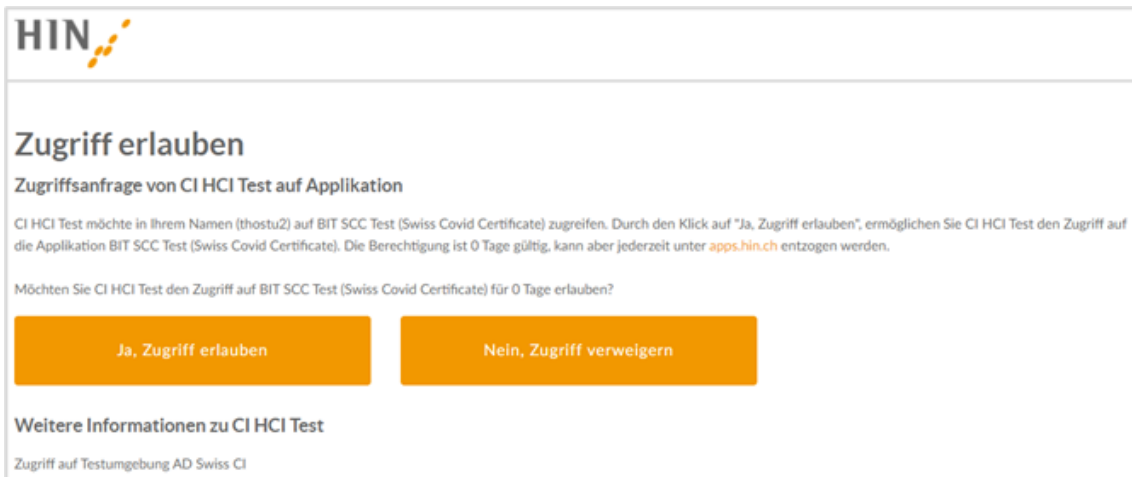
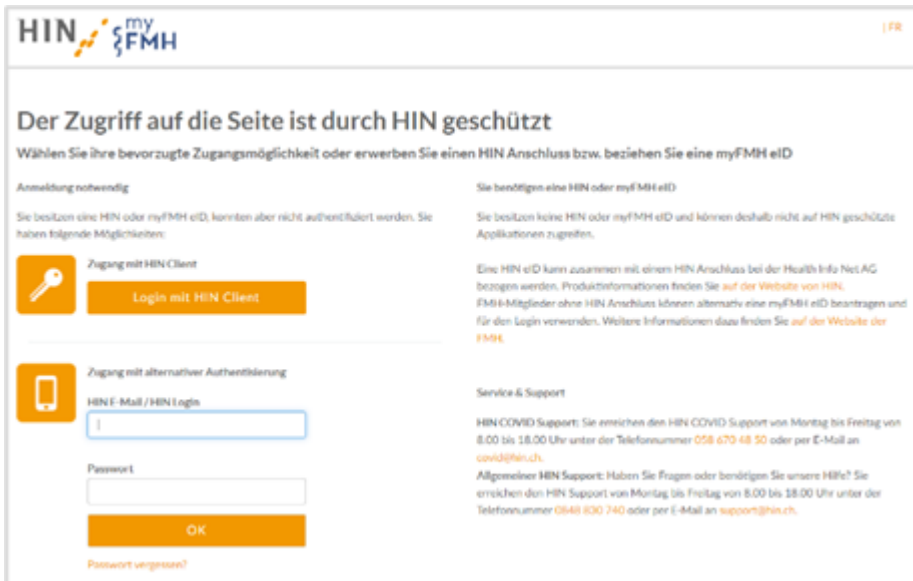
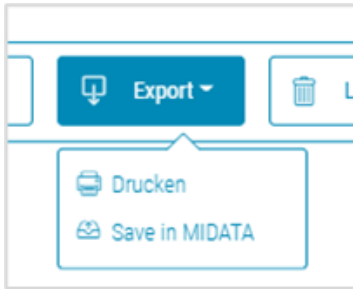
DE: https://download.hin.ch/documentation/oAuth2_Dokumentation_de.pdf

FR: https://download.hin.ch/documentation/oAuth2_Dokumentation_fr.pdf

Example procedure

With the current “Vac” solution, the HIN login is still checked for the authentication level before a certificate is created, as a personal HIN eID (EPR or classic) and access authorisation are required for this process. The HP is automatically connected to the HIN login page. After login, the user must allow access to the third-party application. After this confirmation, the HP is redirected back to Documedis. The login is then valid for 24 hours. After that, a new authentication is necessary.

Mockups HIN login:



5.5.1. Register HP

As described in 2.9.2. HP onboarding and authentication, the HP will access the vaccination portal through Documedis using his HIN login.

Pre-condition

- HP has a HIN eID
- HP's identity has been verified by HIN
- HP has access to Documedis

New HP in MIDATA (first access)

- HP accesses the vaccination portal via Documedis
- MIDATA authentication system automatically redirects the HP to the HIN login page
- HP's credentials are verified by the HIN server and a SAML assertion is generated
- If a HIN session is already active, HP is not requested to enter his credentials again
- The MIDATA authentication system verifies the SAML assertion generated by the HIN server
- The MIDATA authentication system extracts from the SAML assertion the required attributes (HIN ID, GLN, last name, first name, email, etc.)
- If the HIN ID is not present in MIDATA, a new user account is automatically created. The required attributes are retrieved from the SAML assertion and stored in the MIDATA HP account
- The HP is now authenticated on MIDATA and can perform standard operations like search and retrieve patient data (to which he has access)
- Patients may give access to their vaccination data to authenticated HPs

Existing HP in MIDATA (subsequent accesses)

Similar to the previous use case, with the exception that if the HIN ID contained in the SAML assertion generated by the HIN server is already present in the MIDATA system, the HP is authenticated and redirected to his main page (his primary system or Documedis).

Attributes returned by the HIN SAML assertion

Attribute name	Example	Used in MIDATA
X-HIN-ASAS-UserId	31393	X
X-HIN-USERTYPE	Personal	
X-HIN-POSTALCODE	2502	
X-HIN-LOGIN-NAME	hwenger1	
X-HIN-POSTAL-CODE	2502	X
X-HIN-ADDRESS-1	Höheweg 80	X
X-HIN-ORGANIZATION	Berner Fachhochschule	X
X-HIN-MAIL	hanspeter.wenger@hin.ch	X
X-ASAS-UserId	31393	
dateofbirth	1964-09-29+01:00	X
X-HIN-COUNTRY	ch	X
X-HIN-GIVEN-NAME	Hanspeter	
GLN	7640166732204	X
X-HIN-PERSON-CODE	1	
X-HIN-AUTH-METHOD	ALTERNATIVE	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Hanspeter	X
X-HIN-TEST-CODE	1	
X-HIN-SESSION-IDENTIFIER	6dd310ac480aqwltWndtdeyRgPLI YrEkP40w/7ieRadRz7MizXeJd8E =	
X-HIN-LOCATION	Biel/Bienne	X
X-HIN-COMMON-NAME	Hanspeter Wenger	
X-HIN-USEREXTID	31393	
X-HIN-INSTITUTION-CODE	1	
X-HIN-LANGUAGE	de	X
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Wenger	X

X-HIN-EAN-NO-MEDICAL	7640166732204	
X-HIN-SURNAME	Wenger	
NameID	HIN_2f0c6c13f5ad746c...	X ⁽¹⁾

(1) NameID

NameID is described in the *Anhang 8 der Verordnung des EDI vom 22. März 2017 über das elektronische Patientendossier (SR 816.111.1)* as

“randomly chosen unique identifier that SHALL be persistent and confidential outside the IdP-RP-System and never presented neither to the claimant or its agent nor to third-party-systems”

MIDATA will use NameID as the “secret” that is required on the server to decrypt HP’s private key. NameID will not be stored on the MIDATA server, making it impossible for hackers to decrypt personal data, in case of a security breach on the server.

5.6. Patient app to CDS

The business logic between the patient web app, Documedis and MIDATA.

There is no interface between the patient app and the CDSS in the MVP. The CDS service is reserved for the HP. Only the results stored in MIDATA can be viewed by the patient.

The web app should be hosted on a “public” web server. All requests from the web app should be diverted to an “internal proxy server” and then to Documedis and MIDATA servers according to information needed.

All requests go through Proxy server and transferred via VPN to Backend servers, and return information to apps too. This secures all accesses to backend servers. As MIDATA already has a kind of proxy server through its load balancer, there is no need for an additional one. All communication should be in SSL mode “encrypted” from B2C side to proxy server.

The main APIs to be used in the patient app are:

- Patient profile API “read”
- Patient profile API “create and update”
- Patient immunization dossier API “read” all records
- Patient immunization dossier API “create and update” one record at a time
- Patient grant authorisation HP API
- Patient delete authorisation HP API
- Patient list of authorized HP API
- ... list not exhaustive....

The app interface will be structured in several components (tabs):

- Main tab: “what do you want to do?”:
 - Add vaccination record
 - Import old vaccination record
 - Grant authorisation to HP
- Vaccination records tab
- Calendar of future vaccine recommendations tab (by CDS)
- Authorized HP list tab
- Patient profile tab
- Parameters tab

Like the HP app (see next chapter), the patient web app anonymises the vaccination data set prior to sending them to the CDS (note: if FHIR resources are used in the API, they should not contain any link to the patient or patient ID).

5.7. HP app to CDS

The CDS functionality will be integrated into the HP app. This means that the HP can document vaccines via the HP app and also use the CDS functionality.

The detailed concept for integrating the CDS functionality into the HP app is currently still being developed. It is planned that the questionnaire for the vaccination CDS will be integrated into the tab “Vac” in Documedis and that the results can also be retrieved in Documedis.

eMediplan Rp PMC Care Covid **Vac** PCA LINDAAFF CDS EPD

Dora Graber
23.11.1945

Import Export Löschen

Patienteninformationen

Personalien

Ich möchte

- eine Impfung Dokumentieren Hinweis → Dieser Bullet Point entspricht dem Heutiges Vac Tab (Corona + pHs-Impfungen)
- einen allgemeinen Impfstatus abfragen
- eine spezifische Impfung mit Impfstatus abfragen

All data and/or results of the CDS check will be stored either in MIDATA or in the HP's primary system.

Like the patient app, the HP app anonymises the vaccination data set prior to sending them to the CDS (note: if FHIR resources are used in the API, they should not contain any link to the patient or patient ID).

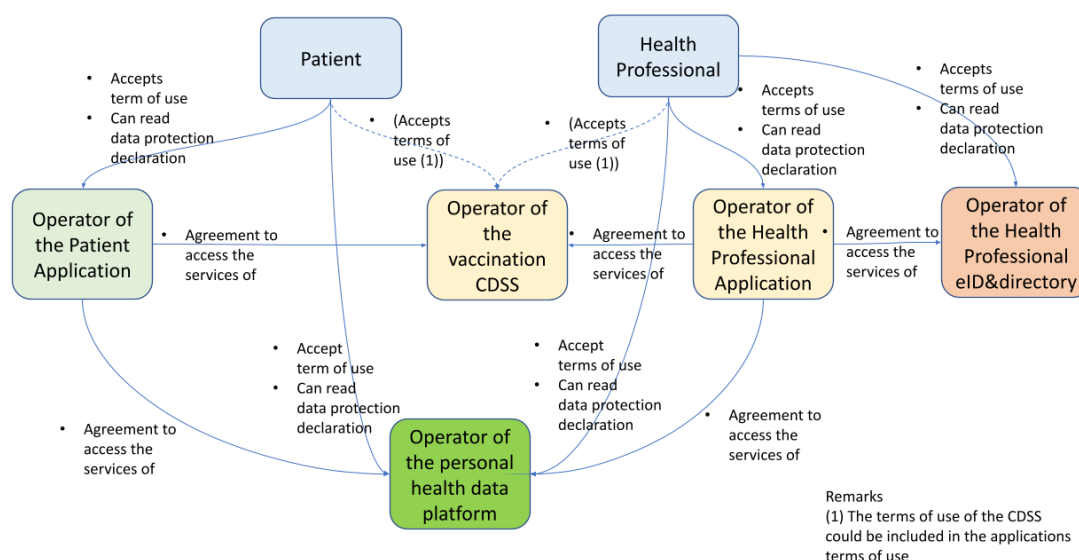
6. Legal

The actors constituting the “vaccination data ecosystem” and their relationships are represented in schema 1 in [chapter 1.2](#).

We see the ecosystem as neither in the control of a general contractor or single actor, nor in the control of a single legal entity like an association or consortium.

We see it rather as the dynamic cooperation of actors offering each other services. We strongly believe this is the most sustainable and adaptable form to operate an ecosystem capable of evolving over time.

To ensure a trustable operation and a clear identification of responsibilities we see the following legal relationship between the actors identified in chapter 1.2



Schema 9: Overview of actors' legal relationships.

6.1. Relationship patient app owner to MIDATA

6.1.1. The MIDATA platform as a secure patient-centric backend

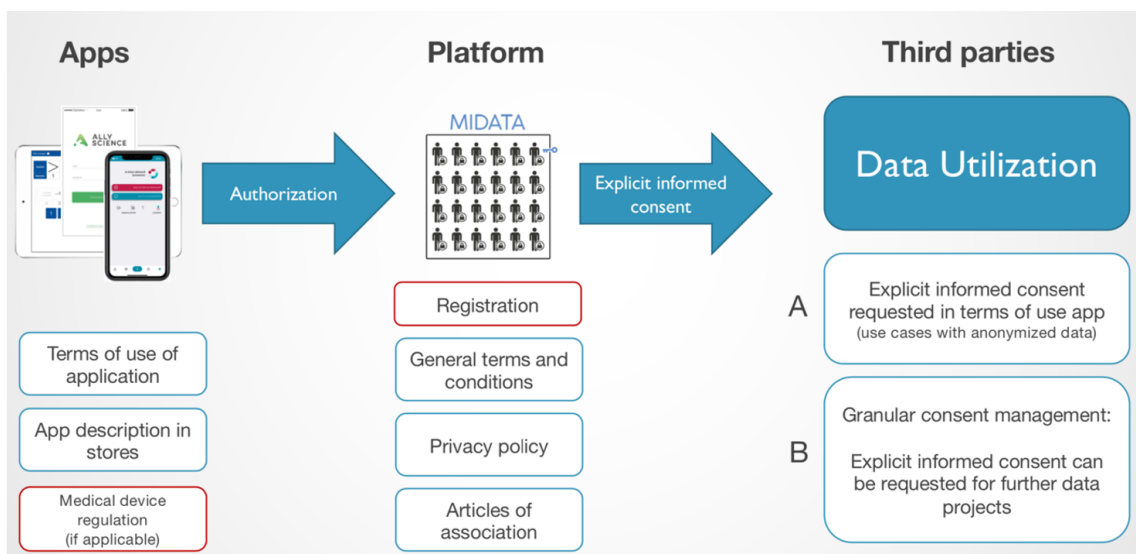
MIDATA Cooperative provides a platform for the encrypted storage of personal data. Patients access their personal data through the web app. Data stored by app users through the app is stored in encrypted data accounts on the MIDATA platform.

App users are account holders of an encrypted data account on the MIDATA platform over which they have sovereign control. Account holders freely dispose of their personal data as follows: MIDATA will only disclose personal data (registration data, content) of an account holder to third parties with the prior explicit and informed consent of the user and

/ or allow them to access the corresponding data. This applies regardless of whether the personal data is passed on in original, encrypted, pseudonymized form or whether it is passed on exclusively in anonymized form. (MIDATA Privacy Policy, Article 6; MIDATA Articles of Association, Articles 4 and 5).

Sovereignty of a user over his data on the MIDATA platform also means, among other things, that the use of the data by MIDATA itself is not possible without explicit consent of the user. This is technically implemented via the granular encryption and key system. The use by third parties is also technically implemented via the key system. For such use, the user's consent must be available and the use must be contractually regulated between MIDATA and the third party.

General framework of data flows and associated contractual and regulatory documents:



Schema 10: MIDATA contractual and regulatory documents.

6.1.2. Relationship patient app owner and service provider to MIDATA

Between patient web app owner and MIDATA Cooperative, a contract concerning app connection to and data storage on the MIDATA platform will be put in place, containing the following elements:

- Description of the relationship between web app owner and MIDATA cooperative
 - Description of app functionality
 - Storage of personal data on the MIDATA platform
 - Stipulations concerning data transfer (e.g., encrypted transmission)
 - Description of the mode of onboarding (acceptance of terms of use and privacy policy patient app by user, registration and acceptance of terms of use and privacy policy of MIDATA cooperative by user)

- Description of the nature of personal data accounts on the MIDATA platform, including data ownership and sovereign control of the account holder
- Description of aspects of data protection and security and compliance.

6.2. Relationship patient to patient app provider

Patients, as users of the patient web app, store their personal data on the MIDATA platform, and they give consent to use of their data by HPs through the consent management system associated with the MIDATA platform. Therefore, the user onboarding process is structured in the following way:

1. user accepts the terms of use of the patient app (purpose of the app, consent for the use of data occurring within the scope of app use).
2. registration on the MIDATA platform with acceptance of the general terms and conditions and privacy policy of the MIDATA platform.

The terms of use of the patient need to include:

- Description of the app functionality
- Description of the mode of data storage in personal data accounts on the MIDATA platform
- Description of the consent management (i.e. the app allowing the user, by way of the MIDATA platform consent management) to grant granular consent to sharing of his/her data with individual HPs

The general terms and conditions and privacy of the MIDATA platform for account holders are preexisting. The current general terms of use and privacy policy will be updated shortly to a version which includes compatibility to the GDPR. It is not expected that the general terms of use and privacy policy will have to be adapted for the vaccination data ecosystem use case. It is however recommended that they undergo a legal review concurrent with the finalized terms of use of the patient app.

The links to the MIDATA *Articles of Association*, *General Terms and Conditions* and *Privacy Policy* are available under [11.4](#).

6.3. Relationship patient to MIDATA

As described above ([6.2. Relationship patient to patient app provider](#)), patients, as users of the patient web app, store their personal data on the MIDATA platform, and they give consent to use of their data by HPs through the consent management system associated with the MIDATA platform. By registering on the MIDATA platform, they become account holders of an encrypted personal data account on the MIDATA platform. As account holders, they are sovereign owners of the personal data which is stored in their data account and need to give explicit consent for use of their data by the MIDATA

cooperative and by third parties, for use of the data in nominal, pseudonymized or anonymized form. Rights and responsibilities of the account holders are codified in the Articles of Association of the MIDATA Cooperative as well as in the General Terms and Conditions and Privacy Policy of the MIDATA Platform.

During onboarding, the patient registers on the MIDATA platform with acceptance of the general terms and conditions and privacy policy of the MIDATA platform, or selects his/her pre-existing MIDATA data account.

The links to the MIDATA *Articles of Association*, *General Terms and Conditions* and *Privacy Policy* are available under [11.4](#).

6.4. Relationship HP app owner and HP to MIDATA

Between the HP app owner and MIDATA Cooperative, a contract concerning app connection to and data access on the MIDATA platform will be put in place, containing the following elements:

- Description of the relationship between HP app owner and MIDATA cooperative
 - Description of HP app functionality
 - Access of HP to patient data on the MIDATA platform
 - Stipulations concerning data transfer (e.g., encrypted transmission)
 - Description of the mode of data access (registration and acceptance of terms of use and privacy policy of MIDATA Cooperative for HP by HP)
- Description of the nature of personal data accounts on the MIDATA platform, including data ownership and sovereign control of the account holder
- Description of aspects of data protection and security and compliance

HP registers for an “HP account” on the MIDATA platform. Upon registration, HP needs to accept the *General Terms and Conditions* and *Privacy Policy* of MIDATA Cooperative for HP. The MIDATA platform allows to serve specific terms for HP connecting to the MIDATA platform as HP users of the HP app. These terms will be adapted for the vaccine ecosystem use case from the existing HP user terms. Onboarding of the HP to the MIDATA platform occurs through the HP app, user authentication being supplied via HIN login (see [2.9.2. HP onboarding and authentication](#) and [5.5.1. Register HP](#)).

6.5. Relationship patient app provider to CDSS provider

It has not yet been conclusively clarified whether and to what extent CDSS will be integrated into the patient app. If a full integration of CDS into the patient app is intended, this still needs to be clarified (see [9.2.2 CDSS for patients](#)).

6.6. Relationship patient/HP to CDSS provider

The HP and the patient use the CDS service to receive vaccination recommendations. To do this, they enter the relevant data and the CDS processes the entries. No data is stored at the CDS provider. In order to use the service, the HP/patient accepts the terms of use of the CDS service (consent to the use of data generated in the course of service use). The terms of use of the CDS correspond to those of Documedis.

The general terms and conditions and data protection provisions of Documedis are already in place. The current General Terms and Conditions of Use and Privacy Policy will be updated to a new version shortly. It is not expected that the general terms of use and privacy policy will need to be adapted for the use case of the vaccination data ecosystem.

Appendices:

- Current Terms of Use of Documedis (original language German)
- The Terms of Use apply to both CDS and Documedis

6.7. Relationship HP app operator to CDSS operator

As the CDS functionality will be part of the HP app, no contract or terms of use are necessary here.

The integration of the CDS into Documedis is currently still in the concept phase. The plan is for the CDS service to be integrated directly into the existing “Vac” functionality. However, this has not yet been finally decided. It is clear that CDS will be integrated into Documedis. The terms of use of Documedis (HP app) therefore also apply to CDS.

6.8. Relationship HP to HP app operator

The HP uses the HP app operator service to document the vaccine (immunization administration). To do this, they enter the relevant data as explained in the user stories. No data is stored at the HP app operator. In order to use the service, the HP accepts the terms of use of the HP app operator service (consent to the use of data generated in the course of service use). The terms of use of the HP app operator correspond to those of Documedis.

The general terms and conditions and data protection provisions of Documedis are already in place. The current General Terms and Conditions of Use and Privacy Policy will be updated to a new version shortly. It is not expected that the general

terms of use and privacy policy will need to be adapted for the use case of the vaccination data ecosystem.

6.9. Relationship HP app operator to HP eID operator

The HP app operator has an existing contract with the HP eID operator HIN. By this contract, the HP app operator has accepted the terms of use from the HP eID operator.

A brief overview of the services that the HP app operator uses from the HP eID operator:

- Assurance of authorized access through authentication levels and the definition of attributes.
- Differentiated access rights through individual user administration and automatic user authentication
- Support for profile management and ensures updated master data
- User access support
- Simple, secure and transparent integration into the existing processes of the healthcare institutions.

Based on this partnership, the HP app operator offers login via HP eID operator.

The links to the HIN *General terms and conditions* are available under [11.4](#).

6.10. Relationship HP to HP eID operator

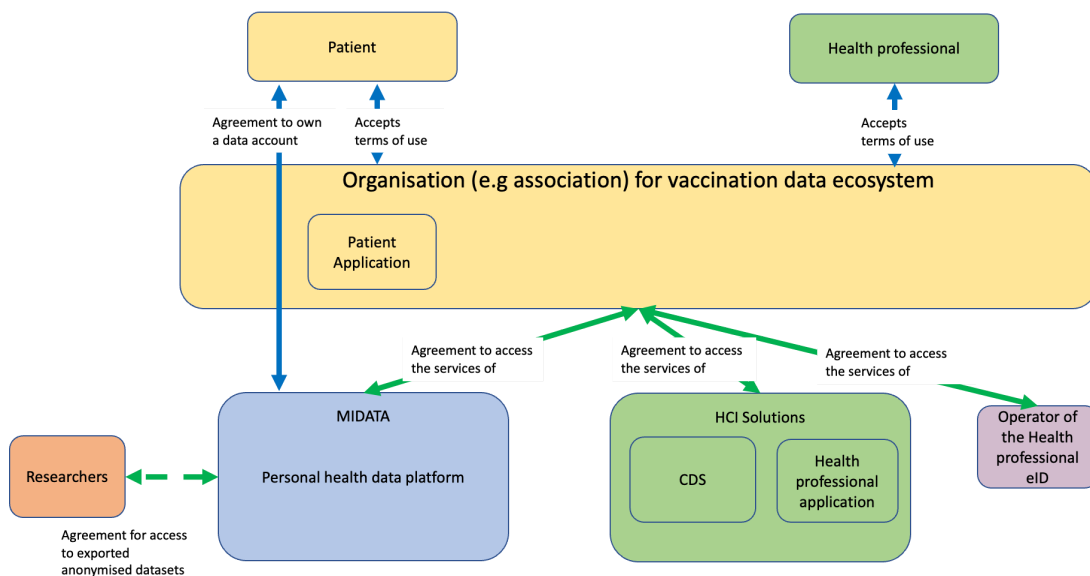
With the HIN membership (HP eID operator), HIN participants receive an electronic identity (eID) according to the laws of the EPDG. The Federal Act on the EPR stipulates that every health professional must have a secure electronic identity to access the EPR (EPDG, Art. 7). The associated ordinance requires secure identification of the person and verification of professional qualification when issuing eIDs. The identities must be issued by a certified identity provider (EPDG, Art. 11). The personal identities of HIN form the basis of data protection-compliant electronic communication and fulfill the requirements of the EPDG. The HP must therefore accept the terms of use of HIN.

In connection with MIDATA: a redirect to the HP eID operator will be executed from the HP App. After the HP eID operator confirms the successful login, the HP must allow access to the third-party application (in this case MIDATA). After this confirmation, the HP is redirected back to the HP app. The login is then valid for 24 hours (it depends whether it is about a personal login or not).

The links to the HIN *General terms and conditions* are available under [11.4](#).

6.11. Alternative organizational and legal setup

Building upon the network of bilateral contractual relations detailed above, the framework could alternatively be set up using a central supporting organization (“Trägerorganisation”), e.g., an association, which would issue and operate the patient app. Such an organization could form the patient and HP facing front and could constitute the party entering many of the contractual relationships with the different actors described above.



Schema 11: Overview of legal relationships with central supporting organization.

7. Security by design

7.1. General security principles

Security and data protection are essential components for this project and as such, they will be treated with the highest priority. Security principles can be fundamentally decided by looking at the three central aspects of security: confidentiality, integrity and availability.

Each of these aspects is important in itself and should always be well implemented. However, there are cases where different aspects are in direct competition with each other, and improvements in one aspect might lead to deterioration in another aspect. For this reason, it makes sense to prioritize the aspects for the vaccination data ecosystem use case:

Confidentiality

The Data Protection Act clearly classifies medical data as particularly worthy of protection. As vaccination data is part of this category, we deem confidentiality of information the most critical security aspect in the context. Moreover, recent history has shown how confidentiality breaches can majorly undermine solution providers' reliability and public image and permanently compromise their ability to exist. To follow this principle, strict measures on data confidentiality must be implemented, specifically patient's data, including demographic and contact data, must only be accessible by HPs which have been explicitly authorized by the patient itself. The consent management solution combined with strong data encryption mechanisms, both provided by the MIDATA platform, are core architectural elements for the achievement of high data confidentiality standards.

Integrity

Protecting data against intentional or unintentional modification comes in a close second. Ensuring the accuracy and consistency of the data over the whole data lifecycle is one of the most important aspects to take into account when protecting the health of the data subjects. For this reason it is important to identify, already in the design phase, validation mechanisms (e.g., based on checksum) as well as traceability solutions (e.g., audit trails).

Availability

It is quite conceivable that data availability violations can lead to life-threatening situations. However, considering the low criticality of the particular vaccination booklet system, we can safely rate data availability less critical than confidentiality and integrity. Nevertheless, redundant architecture and data backup plans are critical parts of the solution design.

In addition to that, data security implies management of the data based on security aspects, regular verification that security is continually assured, and protection against data loss.

Due to the decentralized nature of the ecosystem approach, it is important that the

involved stakeholders and partners do agree on a common framework and governance policies to regulate and monitor the different aspects related to data protection and security.

A management system for data protection and security should be put in place.

The main aspects the management system should include:

Risk Management	Including a thorough catalog, periodically reviewed, listing all foreseeable risks that might impact the solution, grouped by their impact and probability. Remediation plans should be produced and maintained. In case a risk is accepted, the decision should be properly documented.
Policies for information security	All responsibilities for information security must be defined and assigned. Duties and responsibilities with potential for conflict must be segregated to reduce the risk of unauthorized or unintentional modification and abuse. As well the assignment of authorizations must be limited to business requirements with a clear review process in place.
Monitoring and incident management	Continuous monitoring of critical systems and detection of anomalies. Clear notification, escalation and reporting procedures must also be in place in case an incident or an attack is detected. In particular on this point, in line with GDPR, in case of data breach, users must be promptly informed.

Main safety and security features:

- The platform is hosted in Switzerland, on redundant servers.
- Yearly external security audits.
- Data are encrypted using multi-level encryption, allowing granular sharing of specific data sets.
- Account holders may encrypt their access key, precluding server-side data breaches.
- Two factor authentication available.
- Data traffic from and to server via HTTPS.
- Connection and all safety tokens using perfect-forward secrecy.

Specific for MIDATA

Data protection is key to any data science project. It is required by legislation and it is mandatory to build and maintain trust with the data owners. Data protection means in particular allowing access to data only to parties that have received explicit informed consent by the data owners. In addition to that, data security implies management of the data based on security aspects, regular verification that security is continually assured, and protection against data loss. The MIDATA IT Platform enforces data protection by:

- Allowing a citizen to register to the platform and become an account owner
- Authenticating each data owner using the platform
- Securely managing the data of each data owner

- Allowing a data owner to share data with another user or with a third party conducting a data science project
- Managing the access to the data of each data owner
- Allowing a data owner to delete his/her data
- Allowing a data owner to withdraw from the platform and have all data optionally exported and then deleted
- Identifying each researcher using the platform
- Managing descriptions provided by researchers of each of their data science project as a basis for receiving explicit informed consent
- Managing the consent of each data owner willing to participate in the data science project and sharing part of his data in nominative, coded or anonymized form
- Allowing each participant to withdraw a consent to MIDATA-related aspects of a project. In addition to the services provided by the MIDATA IT Platform, additional organizational measures have been taken like:
 - Identifying users as real persons in order to prohibit fake users
 - Managing the register of the researchers using the MIDATA IT Platform
 - Managing and vetting the MIDATA administrators of the MIDATA IT Platform
 - Review the ethical quality of services by a dedicated ethics committee.

7.2. Logins (identification, authentication)

7.2.1. Lifecycle management

Primary Systems

The participants that are grouped together in the vaccination data ecosystem can change over time and therefore the ecosystem and thus the MIDATA backend platform must be able to deal with the entry of new organizations and the exit of old ones. As these systems need to be authenticated but also authorized it must therefore be possible to grant a system the right to successfully establish a connection and also to remove it again. The data must always be considered in the context of the system anyway. This means that a patient identifier from a primary system must always be interpreted in the context of the corresponding primary system, because the same identifier could also be used in another primary system for another patient. The primary systems should integrate the MIDATA patient ID in their system to enhance patient search. This will be proposed in the pharmacies primary system to accelerate the search. Otherwise the search will have to be done by last name, first name and date of birth.

Identification from application

Once the patient app and account are created, it should be possible on the patient app to generate a QR code or show the ID number of the patient in the MIDATA platform to enhance the search of the patient by HP when fetching the patient dossier.

7.3. Autorisation for HP

In the context of this project, we will consider only authorisation of patients granted by scanning the HP QR code in the patient app to a single HP (as physical person in the legal sense).

7.6. Data access management

In this project, access granted by a patient to an HP only concerns vaccination data types (see [3.2.1 CH VACD](#)).

7.7. Data encryption

In the digital world, one method of ensuring security in terms of integrity and confidentiality is cryptography. This is very complex and therefore also very susceptible to incorrect manipulation. It is therefore recommended that the cryptographic methods used and their processes be regularly checked by experts. This could also be carried out by a specialized institution in conjunction with a penetration test:

Encryption of patient data at rest, in transit and in processing, especially those classified by law as requiring special protection. MIDATA provides as core functionality an encryption mechanisms that is described as follow:

On the MIDATA IT Platform, each data item is stored and managed as a single record. Each record is encrypted with a first key, which is stored with other similar keys in an access permission set. This access permission set is encrypted with a second key. In a third step, this second key is encrypted with the public key of the data owner. A data owner willing to access his/her data will use his/her primary key to decrypt the second key that allows him to decrypt and read the access permission containing the keys to finally decrypt, access and read the data. All those operations are triggered by the user but executed by the MIDATA IT Platform, thus hiding this complexity to the user. For a data owner giving consent to share data (referenced in one of his access permission sets) with a researcher or with another user, the second key which had been used to encrypt that access permission set will then be encrypted with the public key of the researcher or of the other user. In this way the researcher or the other user uses his/her primary key to decrypt the second key which allows him to decrypt and read the access permission containing the keys to finally decrypt, access and read the data. Security audits are run by external independent and recognized security expert organizations on an annual basis. These audits check that no unauthorized access to the platform and the managed data is possible. Some of those intrusion tests are run with no user login available to attempt access to any data, other tests are run with a user login with the intent to access more data than allowed.

7.8. Network security

Specific measures should be in place to minimize the possible surface of attack. In this context, network security plays a particularly crucial role.

- System hardening
- Deactivation of all unnecessary and not utilized network interfaces
- HTTPs and SSL for all the connections
- Where possible enforce client side certificates
- Implement network segregation of different logical layers (i.e. databases in a different network zone than public available API) should be evaluated
- Segregate, possibly physically, different infrastructure environments serving different purposes (Production, Demo, Testing, Integration).

7.9. Log files / Audit logs

Audit logs must be created to record significant user and administrator activities, each processing of the data, system messages, errors, and information security incidents. In principle, logs should report events terminated with success, but also of the ones that have been rejected or terminated with an error. In particular, the following events should always be logged and present a valid timestamp:

- System authentication (login/logout)
- Search of a patient
- Access or attempts to access to patient's data
- Generation and withdrawal of consents
- Change of authentication and communication means
- Data export requests

Log entries should at least report:

- Event type - possibly with a unique identifier
- Event timestamp
- Active participant identification
- Audit source identification
- Participant object identifier
- Event Outcome Indicator

The log data must be backed up in a timely manner and protected from unauthorized viewing and modification. Retrospective changes to recorded data logs should be easily recognizable and traceable. This must be valid also for the audit trails of admin activities.

Audit logs must be included in the backup and archiving procedures and their retention period should be clearly defined and be, in line with the applicable regulatory requirements.

Active logging, in combination with monitoring systems (see [8.7. Monitoring, alerting and escalation procedure](#)), should also be utilized to detect activity outside of typical or expected patterns suggesting anomalies. These systems should be able to detect as early as possible attacks and intrusions into the infrastructure or the outflow of data. It is therefore crucial to establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.

7.10. Testing

Secure development policy

Specifications for the secure development and maintenance of applications must be created and continuously adapted to current threats. In particular, security shall not be considered an add-on but an integral part of the application's functionalities.

For instance, automated pipelines should check that code is robust, formatted correctly and secure. This should ensure that throughout its lifecycle, the software is checked against bugs, misconfigurations or incorrect use of encryption or encoding.

Secure development environment

It must be ensured that the code versions and configurations of the different environments (for production, integration and test) are stored separately from each other. The source code must be protected against unintentional modification, copying and loss.

Besides the security aspects that must be embedded in the development pipeline, testing activities should include the following four main categories:

Unit test: narrow scope, intended to verify that small functionalities are implemented as specified. These tests are performed directly by the programmer with the intention to reduce the number of bugs observed downstream.

Integration test: system scope. Different components are tested together with the intention of replicating a whole set of application functionalities. These tests must be run in a "production-like" environment specifically dedicated for integration testing and should involve development teams from all the components involved in the ecosystem.

Regression test: narrow and system scope. These tests are particularly important in our case as they are intended to verify that previously working functionalities are not compromised by the introduction of new code or modifications of existing one. Similarly to integration testing those tests require the involvement of cross-organizational teams.

Acceptance test: focused on the verification of the business requirements, those tests can be performed in the presence of final users representatives or other main stakeholders.

7.11. Security audit

Web systems with sensitive content are extremely exposed and a vulnerability in a system or application can be exploited to compromise data. The environment is constantly changing and new vulnerabilities are found every day, which can also affect the vaccination data ecosystem. In sensitive areas we therefore recommend to perform periodic vulnerability analysis and penetration tests according to the following scheme:

- Periodic vulnerability analysis and reporting (recommendation monthly, report at least 1 time per quarter)
- Remediation of vulnerabilities by specialized teams according to criticality and territory
- Once a year an independent external penetration test has to be performed
- Monitoring and log file retention period (at least 1 year) for forensic evidence

As a systematic evaluation of the security of the system and its compliance with regulations, security audits must be run on a regular basis – it is recommended at least once a year. In addition to regular audits, special security audits should be performed following the occurrence of specific events, such as data breaches, major system upgrades, data migrations, or changes to compliance laws.

To ensure neutrality and objectiveness, security audits must be run by external independent and recognized security expert organizations.

In general, security audits should address the following goals:

1. Identify security problems and gaps, as well as system weaknesses
2. Establish a security baseline that future audits can be compared with
3. Comply with internal organization security policies
4. Comply with external regulatory requirements
5. Determine if security training is adequate
6. Identify unnecessary resources

More specifically security audit should check:

1. Network vulnerabilities (i.e. penetration tests)
2. Security controls (i.e. policies and procedures, four eyes principles, access control lists)
3. Encryption (i.e. SSL, data encryption)

These audits check that no unauthorized access to the platform and the managed data is possible. Some of those intrusion tests are run with no user login available to attempt access to any data, other tests are run with a user login with the intent to access more data than allowed.

8. Operations

8.1. General considerations

The levels of acceptance required to make the system a reliable tool in normal daily business can only be obtained if this is available to all participants around the clock. Because even the most simple functions can only be operated correctly if all central components in the ecosystem are available, these components must be correspondingly designed. Such high availability requirements typically necessitate a redundant design of the most critical components, but also the definition of clear processes and guidelines regarding the delivery and operation of the solution.

As by its nature, the vaccination data ecosystem is composed of independent elements, each characterized by its own lifecycle and operational procedures. It is particularly important that the stakeholders involved in the realization of this solution will coordinate in the implementation of a common framework and governance that can ensure high reliability of the services provided.

8.2. Release management

A particular effort should be directed in the definition of release management procedures to ensure quality while supporting the activities of the product and development teams responsible for the different components.

The distributed nature of the solution proposed poses particular challenges requiring a higher degree of synchronization between the different solution providers.

For instance, the introduction of changes in the MIDATA backend, if not properly managed, could lead to disruption in functionalities offered by the patient app. Release management should therefore be seen as a coordinated effort between the different providers rather than a set of processes managed internally, in isolation.

To facilitate this process, common checklists and automated processes must be implemented to ensure that new software releases are not carrying errors, anomalies, risks nor interferences with other components. More in general it is advisable to implement:

- Clear communication and synchronization processes between product teams
- Aligning roadmaps and release cycles
- Coordinated rollout planning
- Automated processes wherever possible
- Maintaining common testing environments and acceptance testing procedures
- Common checklists before release to production

Related to release management, it is also important to identify common governance for the coordination of change management. Typically a change advisory board with

representatives of the different solution providers controls and coordinates changes in the controlled environment.

8.3. Reporting: indicators and statistics

The following KPI as statistical indicators should be produced monthly:

- number of users of the patient app
- number of immunization records
- number of validated immunization records
- number of immunization recommendations
- number of users of the HP app

As the MIDATA server does not have any way to decrypt the stored encrypted patients' data without additional patient consent, the only way to count the immunization records and immunization recommendations will be to add a global resource type counter at the time of the record creation. The number of resource types created by will be displayed in the app statistics overview accessible by the administrator(s) of the MIDATA platform.

8.4. Service Level Agreement

Designing SLA in an ecosystem environment could be particularly challenging. The main reason is that several solutions contribute to the overall provision of the “service” to the end user. Each of those single solution elements can, in turn, be dependent on several service providers, each with its own SLA. For instance, before being able to define key criteria like response time or service up-time, it is important to survey and carefully review what are the same service levels provided by the different cloud providers, internet providers and other third party service providers involved.

Depending on the business model identified, different levels of SLAs can be delivered. However, it is possible that not all end-user services need to be subject to the same SLA requirement class. It is normally the case that the patient app is offered free of charge in a “best effort” mode, while the HP app terms are regulated within a specific contract. Nevertheless, it is evident that the business critical services provided by the MIDATA backend and the HP authentication services must comply with the higher SLA class available.

More in general SLAs should define:

Availability rate calculated as a percentage on a monthly or a yearly basis (normally not including scheduled maintenance windows)

Incident management indicating the channel of communication (email, phone), support hours, priority levels (see table below in First level support)

As the vaccination booklet functionalities will be integrated within the Documedis product, it is advisable to consider as a starting point for the definition of the SLA the conditions already provided within the Documedis service.

8.5. First level support for all components

First level support should be available to all users (patients and HPs) in normal business hours.

Optionally, it is possible to consider a dedicated support line available exclusively to HPs in case of urgent requests incoming outside normal business hours and during weekends. This can be particularly important in case some of the solution providers involved in the ecosystem already deliver this level of support (e.g., Documedis and HIN).

Some of the main aspects to consider for the establishment of a first level support / help desk service:

- Definition of one common point of contact including website, support email and contact phone (depending on resources availability).
- Preparation and constant improvement of FAQ pages.
These should contain clear instructions to guide end-users through most common issues (i.e. “How do I allow a pharmacist to access my account?”, “Why I cannot find a patient?”, etc.). The goal is to reduce the volumes of support requests and to promote self-service solutions (Tier 0).

Some additional elements that should be taken into account for incident management:

- It is key to compile and maintain a comprehensive inventory of all supply chain relationships, main contact persons and escalation procedures.
- A common ticketing system, accessible by all software providers involved in the ecosystem is highly recommended
- Definition of HelpDesk SOP (Standard Operating Procedures), including common workflows, known issues, escalation procedures and priority matrix.
Following an example of a priority matrix, including possible response time and resolution times:

Incident Severity	Definition	Response Time	Resolution Time
CRITICAL	Critical tickets may prevent a customer from working or cause other devastating consequences. These tickets are often worked first or immediately escalated.	1 hour	4 hours
HIGH	High priority tickets may affect a large number of users (i.e. all iOS users).	2 hours	8 hours
MEDIUM	Medium priority tickets may affect a limited number of users. Users may be able to continue work by applying a workaround.	4 hours	12 hours
NORMAL	Normal priority tickets affect only one or two users and may present an inconvenience, but do not impede work.	8 hours	16 hours

8.6. Second level support for all components

Generally speaking, the second level support is delivered by experienced and knowledgeable technicians that can assess issues and provide solutions for problems that the first level support cannot handle.

Second level support should be provided by each solution provider directly involved in the ecosystem. Each second-level support could be organized independently. However, across organizations, common standard procedures and the same ticketing tool must be implemented. It will be mainly the responsibility of the first-level support to identify to which second-level support forward support requests.

For this particular case, we deem it not strictly required to establish a formal third tier of service support. However, it is advisable for the involved organizations to implement a less hierarchical internal support structure where subject matter experts are involved in troubleshooting components they are directly responsible for. The organization could directly follow the DevOps guidelines.

Moreover, it is expected that more complex incidents will require third-party software/service providers' support (i.e. cloud infrastructure, WAN connectivity, database provider, etc.).

It will be a direct responsibility of the second-level support to handle and coordinate these types of escalation channels directed outside of the ecosystem.

8.7. Monitoring, alerting and escalation procedure

Monitoring systems should be put in place to support the overall operational management of the solution. In particular, monitoring should support functional areas such as: Fault, Configuration, Performance and Security.

Monitoring tools should provide search, visualization and automated alerting features. Facilitating preventive interventions, troubleshooting activities and forensics analysis in case of incidents.

It is recommended that the overall monitoring solution is designed as a combination of log-based and metrics-based monitoring tools.

A **metric-based tool** should be deployed and configured to monitor system resources, infrastructure status, status of the main application agents and overall performances. Here below some of the metrics, grouped by system level, that should be included in the metric-based monitoring tool:

Applications, web servers and databases

- Components/processes running
- Memory partition (i.e. JVM heap, garbage collection, etc.)
- Resource utilization by each component
- Application-specific health checks/reports
- Internal failures and failures of lower layers (i.e. disk full)
- Configuration changes
- For database services specific information like: r/w requests, transactions, connections count, disk queue depth, IOPS, latency, etc.

Operating Systems and Resources

- System info (i.e. uptime, identifier, date and time)
- Available storage
- Number of processes running
- Data read/written and I/O state
- Memory size, allocated and used
- CPU size and utilization
- Disk size and utilization
- Failures related to memory, disk, or other
- SSL/TLS certificate monitoring

Base infrastructure

- HTTP error codes
- Connection requests
- Latency measurements (i.e. request/response)
- In case of load balancers (failures, queue depth, backend healthy host count)
- Common network statistics (i.e. bytes, packets, error, etc.)

On the other hand, a log-based system should be deployed to collect, analyze and correlate logs produced by various systems like for instance, syslogs, application logs (i.e. log4j), server logs (i.e. Nginx, MariaDB, etc.) and platform logs (PaaS cloud provider). The advantage of implementing a log-based monitoring system is that besides the case of troubleshooting issues, logs can be used for analyzing users behavior, identifying bugs or monitoring application specific metrics.

Due to the distributed nature of the ecosystem-based solution proposed, it is particularly important that the heterogeneous systems involved do produce coherent logs which can be easily correlated and linked with each other. For instance a log produced in the patient app (i.e. patient scanning a QR code) must be linked with a log produced by the MIDATA platform backend (i.e. generation of a consent authorization between the patient and the HP). The use of a common NTP (network time protocol) server and the consistent use of session IDs are therefore highly recommended.

Finally, the collected data should then be accessible via query interfaces and reduced in conveniently designed dashboards.

Dashboards can be designed to serve the purpose of various internal groups, serving various purposes like utilization and capacity planning, security control or even trends analysis indicators (i.e. to monitor the impact and usage of newly deployed features).

8.8. Data recovery plan

To ensure business continuity, a systematic backup and archiving mechanism for all central components must be put in place.

With the current configuration, MIDATA represents the layer of persistence, providing storing capabilities for users identities (both patient and HP), patients' personal data, credentials, consents and encryption keys. Other components like the patient and the HP apps are designed to minimize the requirements of data storage, relying mainly on the persistence offered by the MIDATA platform. This design choice drastically diminishes the criticality in terms of data backup for those components. Nevertheless, for compliance aspects it is expected that logs produced by those components are always included in regular archiving/backup processes. The lack of critical data to be recovered does not change the classification of those components as business critical, requiring their availability at all times. Service availability is addressed through system redundancy.

For data recovery the following basic requirements must be met:

- Backups must be performed on a regular basis (ideally several times per day).
- Data is to be archived in accordance with the legal frameworks.
- The content of backups and archives must be protected against unauthorized access. This specifically includes IT specialists as well.
- The backups and archives contain patients' personal data records as well as the collection of all data for logging and auditing purposes as well.
- Regular checks (at least once a year) of the restore functions of the backups created should also be carried out.

9 Categorizations of functionalities

By default, every functionality not explicitly described below is to be considered included in the MVP.

9.1 Not in MVP, optional features

Below are the optional features listed, which could be part of the product but not essential for the current project scope.

9.1.1 User journey “import vaccination data by HP”

Patients could send an electronic copy of their paper vaccination booklet (PDF, photo) or the XML file exported from *meineimpfungen.ch* to an HP to update and validate their vaccination record.

Following constraints must be analyzed more precisely:

- Secure channel to electronically transmit the XML, PDF or photo: patient app, other channel?
- Business model for this service.

9.1.2 Test data

Allow to integrate tests (like Covid or Hepatitis) in future releases.

9.1.3 CDSS for patients

The CDS service can also be implemented in the patient app. In this case, the content and queries must be adapted to the patient. Specialist content (provided to the HP from the CDSS), must be adapted so that it is understandable for the patient.

9.1.4 Notification by CDS

As the nature of the vaccination record is dynamic, the output of the CDS.CE recommendation will not be stored in MIDATA.

On the app of the patient, in the configuration page, there should be a new option called:

- Vaccine notifications, default value active. The patient should be able to deactivate the notification system if he prefers.
- Automatic check for new vaccine: The patient should be able to deactivate the notification system if he prefers.

To avoid changes and new functionality on the MIDATA side, for the MVP, no CDS recommendation will be stored as specified earlier. In any case 2 options of storing data are possible in this case:

- On the MIDATA server linked to patient record
- On the patient mobile (crypted data) accessible by the patient through the web app.

Since this data is not part of the patient's record but only recommendations, compliance might not be an issue. And since this data is generated by a CDS check, the same data can be re-generated anytime through the same process, so no need for back of this "recommandation data".

On the patient web app there should also be a calendar showing all "futur planned" vaccinations on the app recommended by a CDS check. A list that shows chronologically his 2nd dose of tick-borne encephalitis TBE (FSME) in 3 months, or his reminder of Tetanus in x years. This data is filled by the CDS check done on the patient dossier.

When a patient opens the calendar on his web app, the first time an automatic CDS check is launched if the patient has the parameter "automatic CDS check parameter" set to true. This process will fill the vaccination calendar of the patient. Notification could be managed in 2 ways and has to be checked if compliant:

- On opening the app, a notification is triggered on the screen if a new vaccine is due soon.
- An e-mail is sent to the patient's mail account with an information informing the patient: please check your vaccination record app, a new vaccine is due soon. The patient can then open his app and check his next due vaccin. This should be done only if the notification parameter is active.

It should be possible for the patient to launch a CDS check from his App to update this data anytime.

9.1.5 Patient ID with Trust ID or SwissID

To keep the MVP light it has been decided that the patient opens an account without ID verification.

One of the first consolidation of the system should be to enforce that the patient should login with a Trust ID or Swiss ID, so that MIDATA and the whole ecosystem could rely on the identity validation.

The current solution is secure in the way that the health professional can only search for a patient in the MIDATA database having given their consent (see [2.10. Search/authorize/linking patient-HP](#)). But still for the future an identification based on an external eID would be better.

9.1.6 External signature of validated records

As described in [chapter 5.4.3](#), vaccination records validated by an HP will be signed digitally using a FHIR resource *Provenance*. The signature will be MIDATA based.

If an external signature is required, a mechanism like HIN Sign – using the HIN identity (eID) as signature – could be used, although HIN Sign is not yet ready to be usable for record signing (actually, only PDFs might be signed) and the service has high costs (5.- / HP / month).

Another option could be to use a blockchain.

10. Glossary

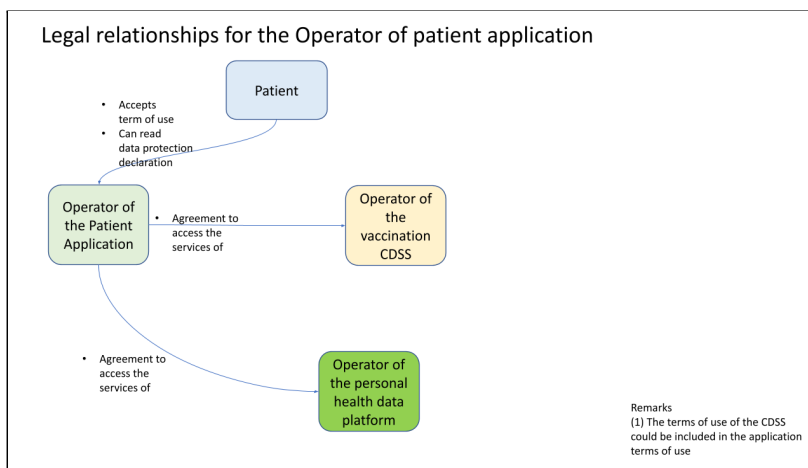
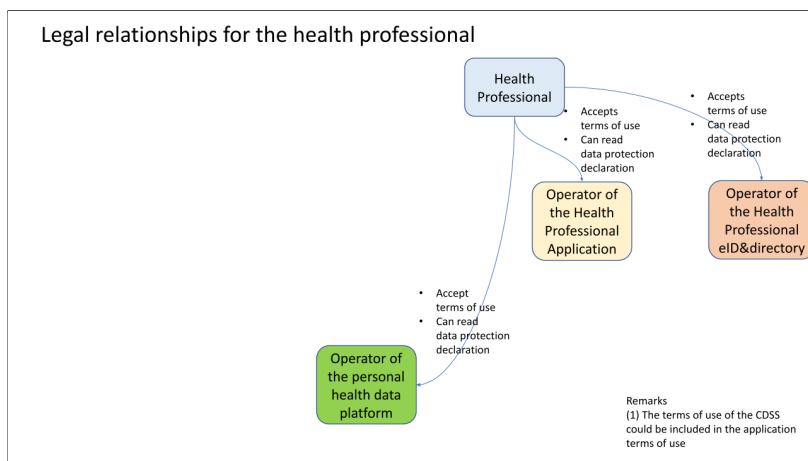
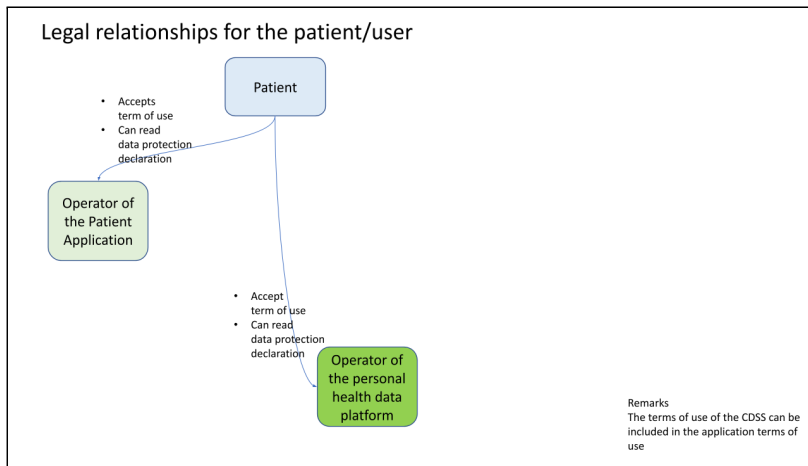
Glossary and acronyms	
Account holder	Person that holds a MIDATA account for storing its personal health data. A health professional needs a <i>MIDATA HP account</i> to access patients' data (with the patients' consent) and might have an <i>MIDATA patient account</i> to store its own health data.
API	Application programming interface.
Authorization	It is an explicit consent provided to a Health professional by a patient, allowing the HP to read, write, edit and validate the patient's immunization administration data stored in MIDATA.
CDS	Clinical Decision Support: health information technology, provides clinicians, staff, patients, or other individuals with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care (Wikipedia).
CDSS / CDS.CE	Clinical Decision Support system, in this context it is the service providing personalized vaccination recommendation based on BAG guidelines.
Customer	In the context of pharmacy visits, it identifies the paying patient. In this text it can be interchanged with the term patient, however, this latter term will be preferred.
Documedis	Web application published by HCI Solutions commonly used by several HPs in Switzerland. It can be accessed either in a native form (web app) or through the integration with primary systems (via APIs).
Electronic vaccination booklet	It is a solution for patients consisting of a) the use of the patient app, b) the ownership of a MIDATA Patient account, c) the management of immunization administrations that together form the vaccination record.
EPR (EPD)	National Electronic Patient Record ("elektronisches Patientendossier (EPD)" in German) as defined by the Federal Act "Gesetzgebung Elektronisches Patientendossier (EPDG)".
FHIR	Fast Healthcare Interoperability Resources: http://hl7.org/fhir/R4
HP / Health Professional	Pharmacist or physician, having in Switzerland a license to practice and owning a valid Health Professional ID.
HP app	Web application used by HPs to access and manage electronic vaccination booklets data. It can be provided as an extension of Documedis.
HP app operator	Company or institution providing and operating the HP app.
HP ID / Health Professional ID	Unique identifier associated with a health professional, e.g. HIN eID.
Immunization administration	Data of an application of a vaccine to a patient for immunization reasons: http://fhir.ch/ig/ch-vacd/immunization-administration-document.html

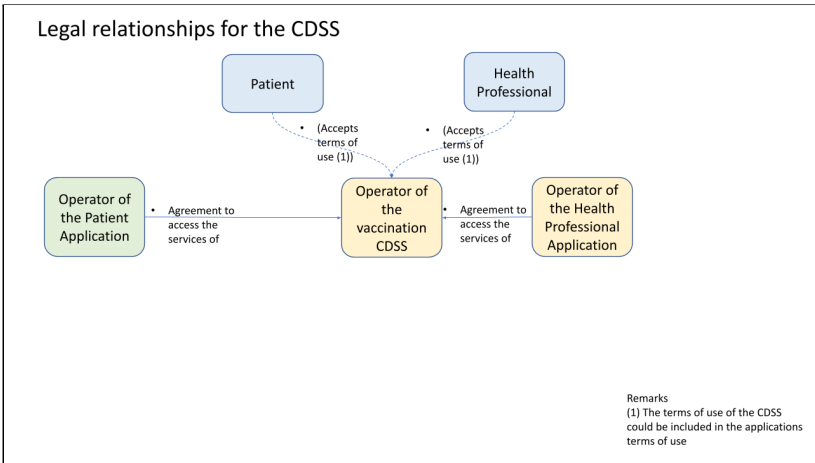
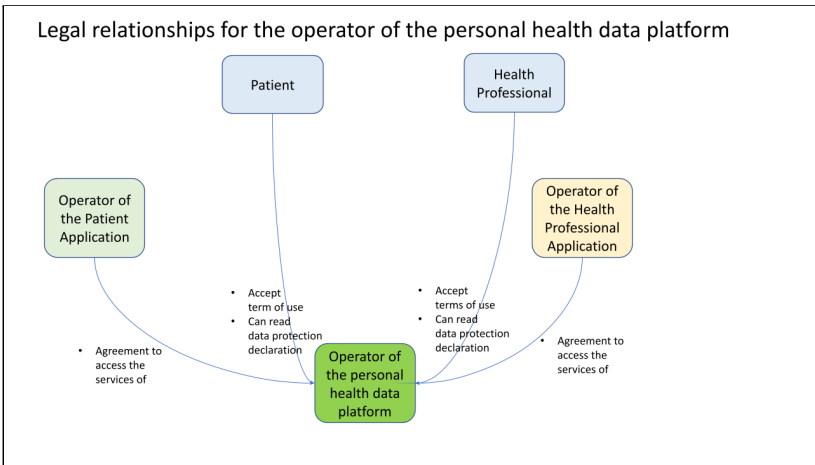
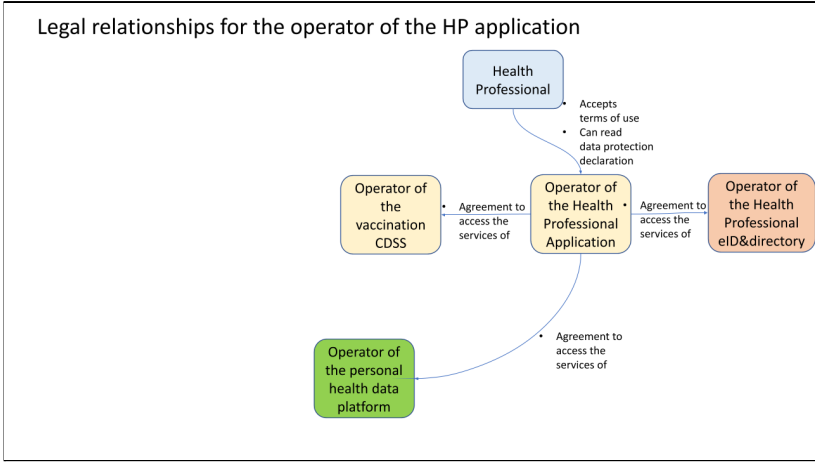
Immunization recommendation	Response containing all immunization recommendations which can be made based on the data delivered by the immunization recommendation request: http://fhir.ch/ig/ch-vacd/immunization-recommendation-response-document.html
Immunization reminder	Reminder to a patient that a vaccination is due soon.
MIDATA HP account	To obtain access to the patient's data, an HP needs to be authorized by the patient via the consent management system provided by the MIDATA platform. A MIDATA HP account is uniquely associated to an HP and linked to his eID or electronic identity (e.g., HIN eID).
MIDATA patient account	Patients as app users are account holders of an encrypted data account on the MIDATA platform over which they have sovereign control.
MIDATA patient ID	Unique identifier associated with a MIDATA patient account and generated by the MIDATA platform.
MVP	Minimum Viable Product: is a version of a product with just enough features to be usable by early customers who can then provide feedback for future product development (Wikipedia).
Patient	A person that is using the electronic vaccination booklet solution independently from his health status.
Patient app / Patient web app	Application used by patients to access and manage their electronic vaccination booklets data.
Vaccination record	In minimum the chapter with the known and applied immunizations: https://fhir.ch/ig/ch-vacd/vaccination-record-document.html
Vaccine	Specific vaccine product administered: https://www.hl7.org/fhir/immunization.html
XML	Extensible Markup Language.
Proof of vaccination	Photo or PDF of a vaccine document (blue or yellow vaccination booklet or written confirmation from a HP).

Main source: eHealth Suisse documentation under <https://www.e-health-suisse.ch>.

11. Appendix

11.1 Legal relationship split by actors for a better readiness





11.2 Requirements and existing eIDs for HP

Requirements for the eID for health professionals

The HP must be uniquely identified
The HP must be securely identified
The HP must be authenticated to perform the required actions according to his /her role and profile
The HP must be authorized to perform the required actions according to his /her role and profile
The authentication of the HP must be performed with at least a two-factor mechanism
The two-factor mechanism must be validated by an official government site

Existing eIDs for health professionals in Switzerland

In addition to the “(Stamm-)Gemeinschaften”, federal law also requires the issuers of the means of identification to be certified for the EPR. These companies have successfully completed the certification process for secure identification (as of August 2021):

Electronic identity	Issuer	Target group and Explanation
HIN eID	Health Info Net AG	For health professionals With the HIN membership, HIN participants receive one or more electronic identities (eIDs). A distinction can be made between personal identities (uniquely assigned to a person) and team identities (uniquely assigned to an organization). Access to the HIN platform is always via HIN eID. In 2019, the HIN eID was certified as the first electronic identity in Switzerland for legally compliant access to the electronic patient dossier (EPR).
TrustID	CloudTrust SA (an ELCA company)	For health professionals offers patients and health professionals a secure and certified digital identity to access the EPR as stated in the Federal Act on the Electronic Patient Record (EPRA).

GenèveID	Canton Geneva	<p>Population and health professionals of the Canton of Geneva</p> <p>Since 2021, the State of Geneva has been offering GenèveID as a new means of certified electronic identification. GenèveID gives access to the Electronic Patient Record (DEP).</p>
VaudID-santé	Canton Vaud	<p>Population and health professionals of the Canton of Vaud</p> <p>VaudID-santé has been developed specifically to access the EPR.</p>

<https://www.e-health-suisse.ch/gemeinschaften-umsetzung/epd-gemeinschaften/elektronische-identitaeten.html>

11.3 Example of a SAML assertion contained in a HIN token

```
<saml2:AttributeStatement>
<saml2:Attribute Name="X-HIN-ASAS-UserId">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">34434</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-USERTYPE">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Personal</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-LOGIN-NAME">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">pjtt31</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-ORGANIZATION">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Health Info Net AG</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-MAIL">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">pjtt31@hintest.ch</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-ASAS-UserId">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">34434</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="dateofbirth">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">1956-10-29+01:00</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-COUNTRY">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">ch</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-GIVEN-NAME">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Rosa</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="GLN"
NameFormat="urn:oasis:names:tc:ebcore:partyid-type:DataUniversalNumbering
System:0060">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">9801000050702</saml2:AttributeValue>
</saml2:Attribute>
```

```

<saml2:Attribute Name="X-HIN-PERSON-CODE">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">1</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-AUTH-METHOD">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">FUTURAE</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="gender">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">FEMALE</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Rosa</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-TEST-CODE">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">1</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-SESSION-IDENTIFIER">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">7d2710ac4b0b5ZdnMrvRB51H66bSopvvqY/FXBrYXeLWQut/knQJ
Z4I=</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-COMMON-NAME">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Rosa Sestak</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-USEREXTID">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">34434</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-INSTITUTION-CODE">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">1</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-LANGUAGE">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">de</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

```

```
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Sestak</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-EAN-NO-MEDICAL">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">9801000050702</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="X-HIN-SURNAME">
<saml2:AttributeValue
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Sestak</saml2:AttributeValue>
</saml2:Attribute>
</saml2:AttributeStatement>
```

Based on the reported SAML assertion, a MIDATA HP account will be created on first login (see [2.9.2. HP onboarding and authentication](#)).

11.4 Terms and conditions of the solution providers

The terms and conditions of the different providers are provided as links or separate attachments:

Solution provider	Link / attachment
Documedis	Terms of use of Documedis (original in German); they apply to both CDS and Documedis https://www.hcisolutions.ch/de/support-academy/downloads-support/compendium/nutzungsbedingungen.php
	Privacy policy of Documedis (original in German); they apply to both CDS and Documedis https://www.hcisolutions.ch/de/support-academy/downloads-support/compendium/datenschutz.php
HIN	General terms and conditions of business https://download.hin.ch/files/HIN_AGB_en.pdf
	Information and framework conditions for electronic data communication https://download.hin.ch/files/HIN_Rahmenbestimmungen_en.pdf
	HIN Access Control Service Service description https://download.hin.ch/files/HIN_Leistungsbeschreibung_ACS_en.pdf
MIDATA	Articles of Association of MIDATA Cooperative (original in German and unofficial English translation) https://www.midata.coop/wp-content/uploads/2019/08/MIDATA_Statuten_20190626.pdf https://www.midata.coop/wp-content/uploads/2019/08/MIDATA_Statuten_20190626_EN.pdf
	General Terms and Conditions for the MIDATA platform https://ch.midata.coop/#/public/terms?which=midata-terms-of-use
	Privacy Policy MIDATA platform https://ch.midata.coop/#/public/terms?which=midata-privacy-policy