LACPASS

Functional and Non-Functional Requirements for a Proof of Concept

Component 1 LACPASS

RED AMERICANA DE COOPERACION SOBRE SALUD ELECTRONICA

BID Banco Interamericano de Desarrollo

REGIONAL PUBLIC GOODS

RACSEL RED AMERICANA DE COOPERACION SOBRE SALUD ELECTRONICA

CENS CENTRO NACIONAL EN SISTEMAS DE INFORMACIÓN EN SALUD

Version 5
March 2022

Introduction

COVID-19 arose at the end of 2019, and, before long, it became a pandemic and gave rise to a series of changes which affected the entire world population and life as we knew it up until then. All contact became virtual, including children's classrooms, work, our social life, and even healthcare.

Every country started designing their own healthcare policies with the main goal of protecting their population. Activities involving mass gatherings were suspended and restrictions were imposed to prevent them, businesses were closed, curfews were imposed. Any measures necessary to avoid exposures.

However, thanks to the advancements in technology and medicine, vaccinations became available almost immediately in previously unseen timeframes, and, slowly, but surely, we are returning to a new normal. Certain laboratory tests are starting to be developed and perfected that will make it possible to identify individuals that are infected so all necessary and appropriate isolation measures can be taken as to avoid the continued spread of the infection.

All of these restrictions continued over time, and the world population started to learn how to co-exist with the virus while still upholding the different preventive measures and respecting any healthcare policies depending on the population's epidemiological situation.

In many cases, there were some countries which started to identify that people should be able to move from one country to another for work, study, or health-related reasons, and they should be able to cross borders between countries while still upholding any necessary precautions.

It is because of these reasons that vaccines have an essential role; they became necessary so that many activities could become possible again and for people to start travelling again. Nowadays, being vaccinated and having negative COVID-19 test results are documents that are required when travelling.

In addition to the certificates mentioned above, the International Patient Summary – IPS, the equivalent of a patient's Clinical Summary which can be exchanged between different countries, makes it possible to know about an individual's health status when facing the possibility of needing planned or unplanned healthcare.

This generated the need to create digital documentation which could be exchanged between the different countries, and which made it possible to certify people's health status.

Goal

The main goal is to exchange information between at least three countries in Latin America and the Caribbean, in a verifiable and secure way, regarding the different types of digital certificates related to COVID-19 and the IPS using the example of the European Union, where the different member countries exchanged information including:

- COVID-19 Vaccination Certificate.
- COVID-19 Testing Certificates.
- COVID-19 Recovery Certificates.
- International Patient Summary – IPS.

For this purpose, the Sanitary and Immigration authorities will have a digital tool which will allow them to learn about the health status of a person in transit between the countries in an accurate and timely manner.

In a scalable manner, the exchange will include information related to the clinical summary of an IPS person so as to obtain an individual's healthcare information not only relating to COVID-19.

To comply with this exchange, a Proof of Concept will need to be carried out where the aforementioned information exchange will need to be conducted with at least three countries in Latin America and the Caribbean.

Context

The exchange of information will be carried out using the same model currently being used by the European Union for the exchange of information regarding COVID-19 certificates, therefore using the same structure presented by the EU Digital COVID Certificate (DCC-EU).

The European Union developed an open-source repository which allows for its member countries, along with more than 24 non-EU members, to exchange information regarding the DCC (Digital COVID Certificate) of individuals:

- Vaccination – to learn how many doses and vaccines the person was administered.
- Test results – to learn the results of a COVID-19 PCR test; a negative result is necessary to travel between countries.
- Patient recovery – to learn if the person had COVID-19, and to have their recovery date.

This is the information that the European Union currently verifies to allow or deny travelers access to the different member countries.

For that purpose, the functional and non-functional requirements for these certificates will need to be defined. The countries wanting to participate in the exchange will need to structure their information as detailed below.

Once the information required for the exchange becomes known, it is necessary to know how the process will be carried out and what safety mechanisms will be used to protect the data.

Several countries in Latin America and the Caribbean considered it necessary to have a similar exchange of information where, during the first phase, they could exchange information regarding certificates between at last three countries in the region, and, later, they could exchange a patient's clinical summary using the IPS profile.

When exchanging information regarding a patient's IPS, the IPS is regulated through the HL7 FHIR[1].

This document describes the functional and non-functional requirements needed to carry out a Proof of Concept to conduct an information exchange related to COVID-19 Digital Certificates.

[1] http://hl7.org/fhir/documentreference.html
https://www.hl7.org/fhir/profilelist.html

Functional Requirements

A functional requirement defines a software system function or its components. A function can be described as an entry, a behavior, or an output, so functional requirements determine how the software behaves.

This document provides a detailed description of the functional and non-functional requirements that will allow for the interoperability of information related to:

- COVID-19 Vaccination Certificate
- COVID-19 Testing Certificates.
- COVID-19 Recovery Certificates.
- International Patient Summary – IPS.

First, we will describe the general requirements that must be implemented for each of the certificates you wish to exchange, and, after that, we will describe the specific requirements for each one of the certificates.

General Certificate Requirements - Details

The system is versatile, solid, and is designed to adapt to the different, diverse systems each country has. The trust framework for the Digital COVID Certificate System is based on a public-key infrastructure which guarantees the authenticity and integrity of the issued certificates using digitally signed quick response (QR) codes.

The authorized certificate issuers (for example, hospitals or laboratories) translate the required information into a QR code. Then, the issuers digitally sign the QR code using an asymmetric cryptographic algorithm and their own private key.

The public keys related to the issuers, which are used to verify the authenticity, integrity, and validity of the digitally signed QR codes, are exchanged via the Digital COVID Certificate Portal. The public key that does not have personal data is transferred between the national digital infrastructures of the member countries (Backend) via the Gateway, and it is then distributed from the countries' backend to a verification software first, then to the mobile devices.

Member countries are allowed, via the Gateway, to exchange their standards of acceptance for the certificates so that, this way, the automatic verification of these rules happens through the verification applications. Thusly, a quick and reliable verification can be carried out for the certificates based on the national standards of acceptance.

Lastly, member countries can exchange the certificate revocation lists (CRL) for either expired or altered certificates.

In order to write this document, which details the functional and non-functional requirements for each of the different digital COVID-19 certificate types, we used information originated from the DDCC which were detailed by the WHO[2], in addition to information from the DCC-EU.

The certificates must contain the following text:
"This certificate is not a travel document. The scientific evidence on COVID-19 vaccination, testing and recovery continues to evolve, also in view of variants of concern of the virus. Before traveling, please check the applicable public health measures and related restrictions applied at the point of destination."

[2] WHO- Digital Documentation of COVID-19 Certificates. Vaccination Status – Technical Specifications and Implementation Guidance. August, 2021.

The requirements found on each one of the three certificate types are the following:

Requirement	Description
General	Universal, timely and affordable access to vaccines, to COVID-19 tests, are the bases to issue them.
General	All certificates must be in a digital or paper format so as to avoid inequalities.
General	An individual can request the certificate in the format they wish to have it, with the option of having the same certificate in both formats.
General	All certificates must be readable for humans and for a system.
General	Access to certificates must be free of charge.
General	All certificates must be issued automatically or upon previous request.
General	A certificate can be issued to another person on behalf of the vaccinated individual, tested or recovered. For example, to the legal guardian of a legally incapacitated individual, or to parents on behalf of their children. Certificates must not be subject to legislation or any other similar formalities.
General	A certificate must contain an interoperable and digitally legible barcode. Anyone reading the code must only have access to the data pertaining the certificate.
General	The authenticity, validity, and integrity of a certificate must be guaranteed using a seal or an electronic signature.
General	All countries involved must have a clear, complete, and timely communication with the public regarding the fidelity, issuance, and acceptance of each of the certificate types.
General	A date must be set for a gradual introduction so that countries that cannot issue certificates in the defined format can still issue certificates that do not yet comply with the standards established. During this period, the rest of the countries must accept the issued certificates as long as they have the necessary information.
Trust Framework	All vaccination certificates must be issued automatically or upon request by the certificate owner.
Trust Framework	All vaccination certificates must have the certificate owner's identity data.
Trust Framework	All certificates must contain information regarding the COVID-19 vaccines that has been administered to the certificate owner, and the number of doses that have been administered.
Trust Framework	They must contain the certificate's metadata in addition to the data related to the issuer, and the certificate's unique identifier.

Trust Framework	For each of the doses administered to the certificate owner, there must be a clear indication of whether the vaccination cycle has been completed or not.
Trust Framework	Vaccination certificates must be issued to individuals participating in clinical trials.
Trust Framework	The security, authenticity, validity, and integrity of all digital COVID certificates, as well their compliance with data protection regulations, are fundamental for them to be accepted in all member countries. For this purpose, it is necessary to have a trust framework in place establishing the regulations and infrastructure for the reliable and secure issuance and verification of COVID-19 certificates.
Trust Framework	The security of personal data must be guaranteed considering the nature of the data.
Trust Framework	A common structure must be established for the certificate's unique identifier.
Trust Framework	A valid, secure, and interoperable barcode must be issued among all countries.
Trust Framework	To guarantee interoperability with international regulations.
Trust Framework	To guarantee that people with disabilities can access the information included in the digital and paper certificates in a format readable by humans.
Trust Framework	They must be based on a public-key infrastructure with a chain of trust which includes the health authorities of the member countries, in addition to other authorities issuing the certificates.
Trust Framework	Exchanging the personal data contained in the certificate must not be necessary in relation to the public-key infrastructure, to the transfer, or to the access. They are only necessary in relation to the public keys related to the certificate issuers and they will be guaranteed using an interoperability gateway created and maintained to this end.
Data Protection	The personal data included in the issued certificates must only be handled with the aim of accessing the information included in the certificate and verifying it to allow for cross-border travels.
Data Protection	The personal data included in the certificates will be handled by the competent authorities of the destination or transit countries only to verify and confirm the vaccination, the test results, or the recovery of the certificate owner. Because of this reason, the handling of personal data must be limited to what is strictly necessary, and the accessed data will NOT be stored.
Data Protection	The certificate issuers will NOT store the personal data necessary to issue it, including the issuance of a new certificate, for longer than what is strictly necessary for its purpose, and in no case for longer than the period during which the certificates can be used.

Data Protection	The certificate revocation lists exchanged between countries will NOT be stored once the validity period has been expired.
Data Protection	The natural or legal person, authority, agency, or any other organism who has administered a COVID-19 vaccination or performed the test for a certificate to be issued will inform the authorities or organisms designated to be responsible for its issuance of the categories of personal data that are necessary to complete the data fields in the certificate.
Verification	The certificate, in combination with the public key for the issuer, must allow for the verification of the certificate's authenticity, validity, or integrity.
Verification	Verification techniques must be used that do NOT require the transmission of personal data included on individual certificates.
Verification	Preserving personal data obtained from the certificate of a person traveling or in-transit is forbidden for cross-border transport service operators.
Verification	The persons responsible for the data must adopt the necessary technical and organizational measures to guarantee that there is an appropriate level of data security.
Verification	The organisms responsible for issuing certificates will be responsible for the appropriate handling of data, thus guaranteeing an appropriate level of data security.
Verification	All certificates must be issued and verified in a secure way.
Identification	All certificates must contain a unique certificate identifier, considering that an individual can have more than one certificate issued in their name.
Identification	The unique certificate identifier must be an alphanumeric sequence, which CANNOT be linked to other documents or identifiers (for example, a passport) owned by the individual
Identification	The aim of using unique certificate identifiers is to avoid handling other personal data, so they are necessary to identify specific certificates.
Revocation	It should be possible to exchange information regarding the certificate revocation list, especially for those that have been issued incorrectly or fraudulently.
Revocation	The revocation list must not contain any personal data except for the unique certificate identifiers.
Revocation	Certificate owners must be informed quickly about the revocation of a certificate and the reasons for the revocation.

Functional Requirement Details – COVID-19 Vaccination Certificate

The following is a detailed description of the functional requirements for the COVID-19[3] Digital Vaccination Certificate.

This description will be split into two stages. First, the requirements related to the Vaccination Certificate will be described for the Continuity of Care scenario, which refers to the moment they were created:

Requirement	Description
General	When a paper certificate is being used, a PHA[4] must implement a process to replace it with the necessary assistive technology.
General	If an offline healthcare computer system exists, the data entry personnel must log in securely to record any information related to the vaccination they could not enter at the time.
General	Any offline healthcare computer system to record vaccinations must include the required content as defined in the basic data set for DDCC:VS[5]
General	Any offline healthcare computer system must be designed to capture quality data including applying data validation rules at the point of data entry.
General	If patient records are stored on an offline patient healthcare computer system available at the moment of vaccination, an authorized user must be able to access a person's record, including their medical history, in accordance with the PHA policies.
General	If an offline healthcare computer system used to record vaccinations is available, it must be possible to perform the following search actions: list, filter, reorder, and export the administered vaccinations history.
General	If an offline healthcare computer system used to record vaccinations is available, it must be possible to develop an export/regular and recurring delivery of data depending on whether an internet connection is available to send them to a different public healthcare records computer system.
General	If an offline healthcare computer system used to record vaccinations is available, then it must be responsible for generating the vaccination data using the FHIR standard.
General	If an offline healthcare computer system used to record

[3] eHealth Network- Verifiable vaccination certificates – Basic interoperability elements – Version 2- 2021-03-12.
[4] Public Health Authority.
[5] Digital Documentation of COVID-19 Certificates. Vaccination Status.

	vaccinations is available, if it is part of the national PKI trust framework, and if it has been authorized by the PHA to sign the vaccination content as a DDCC:VS, then it must record the DDCC:VS using the DDCC:VS recording service.
General	Each service delivery session, center, organization, and context of the healthcare worker for the vaccination's administration event must be defined.
General	If an online or connected public health DDCC:VS generation service is available at the moment of vaccination, then it must be possible to record the vaccine as soon as possible after administering it.
General	It must be possible for the DDCC:VS generation service to accept data from an authorized and connected acceptance point system. If such a system exists, it must be able to accept data transferred from the local data warehouses from the locations where the vaccinations are being administered.
General	The DDCC:VS generation service must be able to represent the vaccination data using an FHIR format.
General	It must be possible for the solution to generate an electronically legible 2D barcode and for the HICD[6] to contain more technically useful information as a final web point to validate the HICD or public key.
General	The DDCC:VS generation service must generate a 2D barcode which must include the minimum amount of unencrypted basic data set contents, in FHIR, for the vaccination, thus providing an electronically legible version of the vaccination certificate.
General	The DDCC:VS generation service must maintain a connection between an HICD, the vaccination data associated with it in a DDCC:VS, any barcode generated from the data, and the private or public key used to sign the data.
General	It must be possible to update the paper certificate for an individual if the certificate is presented during the vaccination process and it has available space.
General	It must be possible to retrieve information regarding the vaccination(s) administered to the person from the content of the DDCC:VS.
Issuance	It must be possible to issue a new paper certificate to a person with the aim of recording the vaccination.
Issuance	The technology must not be necessary for any aspect of the certificate issuance or to update the paper certificate. It must be possible to go through the process completely offline and non-electronically.

[6] Health Certificate Identifier

Identification	Vaccinators must identify the person according to the rules and policies set by the PHA under whose authority the vaccine is being administered.
Identification	It must be possible to register a person if they are showing up for the first time.
Identification	For this purpose, it must be possible to associate a unique HICD across the world with a paper vaccination certificate which records each of the vaccines administered to the person.
Identification	It must be possible to enter or attach the HICD as a 1D barcode to any paper vaccination certificate issued to the person or HICD certificate owner.
Identification	It must be possible to prepare preprinted certificates with an HICD generated beforehand which is at least encrypted within a 1D barcode.
Identification	It must be possible to record the basic data set contents in a paper vaccination certificate issued to the person or DDCC:VS certificate owner.
Identification	Any data that is related to the vaccination, remotely related to the HICD, and the basic data set, must be entered in an electronic format as soon as possible after the vaccine has been administered. The point of care must have a digital system which allows for such a registration to occur.
Identification	If an offline healthcare computer system used to record vaccinations is available, then it must validate and confirm that the entered HICD are unique in accordance with its own data set.
Identification	The DDCC:VS generation service is responsible for issuing the HICD, provided that the HICD can be associated at the moment of vaccination in a timely manner. If the DDCC:VS generation service is responsible for issuing the HICD, it must issue a unique HICD which cannot be repeated in a different paper vaccination Certificate.
Identification	If a pre-generated HICD is being used, or if paper vaccination certificates are being pre-printed, the HICD generation, along with other support technologies, must guarantee that the HICD is not being duplicated within or between other different care facilities, and they must be administered in accordance with the PHA policies.
Trust Framework	All of the data related to the vaccination process must be handled in a secure manner to respect the healthcare worker – person confidentiality.
Trust Framework	The DDCC:VS generation service involved in the vaccination process must guarantee that all data is being encrypted, in transit or elsewhere, to provide end-to-end security for the personal data.

Trust Framework	The DDCC:VS generation service must digitally sign the vaccination data.
Verification	It must be possible to verify the identity of a person using the existing records, if such a verification is mandatory according to local procedures, and it must be possible to retrieve any relevant medical history.
Verification	It must be possible to manually sign the paper certificate and to include the official stamp of the administration center by non-digital means to certify that the content has been recorded by an authorized authority.
Verification	The vaccination certificate, and any validation markers included in them, must be designed to combat counterfeiting and any unlawful use.

The second stage will describe the functional requirements needed for the exchange of Vaccination Certificates

Requirement	Description
General	The paper vaccination certificate must display the HICD.
General	In the places where a paper certificate is being used, the authorities will be in charge of starting the replacement process for lost or damaged certificates using the necessary support technology.
General	A PHA will record any vaccination requests they receive, even if they are done anonymously, so as to have a search history for auditing purposes and to combat counterfeiting, as long as the record respects the data protection principles.
General	There should be a mechanism for country A to notify country B if an allegedly fraudulent certificate from country B has come to the knowledge of country A.
General	One certificate must be issued per person per vaccine, test, or recovery. The certificate must not contain information from previously generated certificates.
General	It must be possible to issue a vaccination certificate to people who were administered a vaccine as part of a clinical trial.
General	It must be possible to issue a vaccination certificate to people who were administered any vaccine doses in a different country, subject to validation by the corresponding health authorities.
General	A PHA must be able to return a vaccination status, as defined by the implementer, to an individual requesting it based on the information they have provided.
General	A PHA must be able to handle individual verification requests or requests sent in bulk.

Identification	An SMS-verification with an alphanumeric HICD must be provided by the PHA as a means to send a verification request or to receive a response with a status code.
Data Protection	The paper certificate, along with any validation markers included in it, must be designed to combat counterfeiting and any unlawful use. Any process which generates a paper vaccination certificate must include elements to help the identifier visually verify that the certificate is genuine by looking at watermarks, holographic seals, without needing any technology.
Data Protection	If a verified is handed a paper or an electronic certificate with a 1D or 2D barcode, they must be able to scan the code and, at the very least, view the HICD coded in the barcode, to visually compare it with the HICD written on the paper certificate.
Data Protection	If a paper or electronic certificate has a QR code in it, and that 2D barcode includes a digital signature, the verifier must be able to verify the signature using the information that has been downloaded beforehand from a DDCC:VS registration service to verify that the certificate is genuine.
Data Protection	A PHA must maintain a PKI to back up the signature and verification process. The lists of validated public keys and the renewal lists are stored on that system and linked to the DDCC:VS generation service to associate the public keys with the HICD.
Data Protection	Each country's certificate authorities must maintain the records in the issued DSC's with the aim of signing vaccination certificates and use any services which allow for them to search for public keys and comparing them with their records to verify their validity.
Data Protection	All communication between the PHA for two countries, or with a supranational DDCC VS[7] registration service must be carried out securely and avoid interferences with the data in transit or idle.
Verification	It must be possible to record all offline verification operations so that, in future phases, when there is an available internet connection, the verification actions can be reviewed and reconfirmed using the data provided by the online DDCC:VS registration service.
Verification	It must always be possible to perform an offline validation of the vaccination certificate. All solutions must be designed so that, if the connection is lost to the solution's online components, there is no need to stop the verification process.
Verification	During the verification process, the verifier has online access to a DDCC:VS registration service managed by a national PHA. They must be able to run queries to see if the HICD obtained from the barcode and public key (if there is a key) included in the paper vaccination certificate are currently valid.
Verification	During the verification process, any solution must send the verification

[7] Vaccination status

	only using the minimum required information for the validation to be completed. That minimum information is related to the metadata and signature of the DDCC:VS.
Verification	When a validation request is received, a national PHA must refer to their DDCC:VS registration service and respond with a status to indicate that the signature key has not been revoked, that the key has been issued by a certified authority, and that the DDCC has not been otherwise revoked.
Verification	A PHA will handle a validation request and respond with the vaccination certificate owner's basic data in accordance with OHA policies, so that the verifier can confirm that the vaccination certificate corresponds to the DDCC:VS owner who presented it for verification purposes.
Verification	A PHA must be able to validate that the requester sending the verification request is an authorized agent, but they must also allow anonymous verification requests.
Verification	It is the final responsibility of the country where the verification process is taking place to decide vaccination declaration is valid or not.
Trust Framework	Any communication between a verifier and a DDCC:VS registration service or any other data service administered by a PHA must be carried out securely and avoid interferences with the data in transit or idle.
Trust Framework	If a verification request is performed on country A for a specific certificate issued by country B or by a supranational entity, country A's PHA must have a way to transfer the request/check the data in possession of the aforementioned authority.
Trust Framework	A member country should establish bilateral or multilateral agreements with the other countries to access the data in the vaccination certificates, in addition the digital signatures of those entities.

Functional Requirement Details – COVID-19 Testing Certificate

The following is a description of the functional requirements a COVID-19 testing certificate must include.[8]

The type of testing required to permit the free movement of people will depend on the country of origin and on the country of destination, where the individual must present a negative COVID-19 test result.

[8] REGULATION (EU) 2021/953 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 14 June 2021

Requirement	Description
General	Creating a list of PCR tests and of rapid antigen tests, which must be validated by all member countries.
General	A COVID-19 testing certificate must be created that can be interoperated between all countries.
General	The type of test that was undergone must be specified, which must be included in the previously defined list.
General	The certificate must include the date when the testing took place.
General	The certificate must display a Negative test result for the test undergone by the certificate owner.
General	The certificate must be issued automatically or upon request by the certificate owner of the diagnostic test.
General	The certificate must include information regarding the NAAT test, or the rapid antigen test undergone by the certificate owner.
General	The certificate metadata must include the certificate issuer's data and their unique identifier.
Identification	It must be possible to identify the results owner in a clear way.
Identification	The certificate must include data related to the certificate owner's identity among the personal data.
Trust Framework	All certificates indicating negative results that have been issued by a member country and identify a test that was carried out that exists in the aforementioned list must be accepted.

Functional Requirement Details – COVID-19 Recovery Certificate

The following table describes the functional requirements related to the certificate[9] which indicates whether or not an individual had COVID-19 within a specific timeframe.

Requirement	Description
General	A certificate must be created for all individuals recovered from COVID-19, which must be interoperable between the different countries.
General	The certificate must contain the date the positive result was detected using a COVID-19 infection test.
General	The recovery certificate must NOT be issued within less than 11 days from the date that the certificate owner obtained a positive result for the infection.
General	The recovery certificate must NOT be issued over a period greater than 180 days from the date that the certificate owner obtained a positive result for the COVID-19 infection.
General	COVID-19 recovery certificates must not be issued for individual's using self-testing diagnoses.
Identification	The owner of the COVID-19 infection recovery Certificate must be clearly identified.
Identification	The certificate metadata must include the certificate issuer's data and their unique identifier.

[9] REGULATION (EU) 2021/953 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 14 June 2021

IPS Profile Requirements

Basic Concepts

The IPS (International Patient Summary) is a consolidated clinical document which provides a set of clinical data which can be used during a non-scheduled consultation with the aim of providing the healthcare professional as much information as possible for the patient's medical care.

This initiative was developed by the European Union and the United States, who set the aim of having a standardized international patient summary by 2020. For the first implementation, in HL7 CDR R", then in FHIR.

The information in the IPS includes:

- Allergies
- Current medication
- Patient problems

In its structure, the CDA displays:

- Patient Information
    - Name
    - Birth Date
    - Sex, among others
- Document Information
    - Creation date and time
    - Latest update date
    - Entity responsible for creating it
- A summary, which contains the patient's relevant clinical data:
    - Allergies
    - Current medical problems
    - Implants
    - Surgical procedures within the past 6 months
    - Current medication

The descriptive information in the IPS data set provides the general layout, with a detailed description of the normative content required to identify and give meaning to the descriptors used to specify each component and subcomponent of the IPS standard.

The following is a detailed description of the functional requirements for the IPS corresponding to the developments in the ISO 27269 regulation.

The corresponding descriptors are:

	Description
Purpose	The meaning and value of the data element.
Definition	A formal description. It is important to point out that this may not be necessary if common use is well known by all parties involved.
Business Rules	A predicate which defines or constrains some aspects of the IPS and always resolves to either true or false. More generally, this descriptor is used to describe business logic.
Missing	The meaning of the absent data and how it should be addressed.
Format	How the data are to be represented if more information is required to clarify data type use.
Inclusion criteria	The rational for including the data element within this document (consistent with the IPS scenario).
Currency	Temporal recommendations for ensuring data are the most relevant for both planned and unplanned care.
Examples	Brief explanation regarding how a particular data element is used in practice.
Notes	Further description related to the data elements; for example, if “optional” or “conditional” requires a more detailed explanation or some contextual information is required. For some coded elements, examples of concepts used for valorizing the element are provided.

The order of the IPS data blocks fall into three different categories:

Descriptive Hierarchy	**H0**	**H1**	**H2-H7**
IPS Data Transfer Object	IPS Document	All possible IPS and the Non-IPS components are identified.	Further details are provided within the IPS Data Blocks' clauses.
IPS Data Blocks	-	Individual IPS Sections, IPS Attribute Collections.	Hierarchical description of the data elements.

The following types are identified within each of the categories:

- Non-clinical data
- Clinical data
- Metadata

It is worth mentioning that, in practice, it is recognized that individual attributes might appear in different categories depending on dynamic use rather than static classification.

Functional Requirement Details – IPS – General

The following is a detailed description of the functional requirements related to the IPS[10].

Requirement	Description
Structure	The IPS has three clinical components: ● Intolerances and allergies ● Medication Summary ● Issues If there is no information available, the included data element must contain a value that indicates the reason why the data was omitted.
List	The formal lists make it possible to support any business rules with precision, conciseness, and legibility.
List	It can be an empty list or a container waiting for its content.
Reference	It is a means to provide a directional link from a source element to a target element.
Reference	Can be internal (that is to say, they are included in the patient's clinical summary) or external (that is to say, referring to objects found somewhere elses).
Reference	Depending on the reference and the type of object, different types of information can be requested: a URL, a set of identifiers, etc.
Coded element	An element which represents a single concept usually provided by providing a reference to external code systems (terminology, ontology). In case of exceptions, it might be defined by providing the text.
Date/time	Can be a complete or partial date.
Date/time	The dates must be valid.
Date/time	If no additional restrictions have been specified, at least one whole year must be specified.
Date/time	The time must be provided.
Date/time	The time zone must be included.
Name of the organization	The names of the organizations must be represented as a simple chain.
Name of the organization	In cases of non-alphabetical representations of names, at least one alphabetical representation must be provided.
Telecommunications	Provides detailed information regarding telecommunication addresses, whether from the organizations or otherwise.

[10] ISO 27269:2021(E)- Health informatics – International patient summary – First Edition 2021-04

Telecommunications	At least one phone number or email must be provided.
Telecommunications	Both can be provided.
Text	The means of transmitting textual information about something. This may range from a medical directive to a medication statement, or a narrative text.
Text	Can include language with or without format.
Text	Is subject to human interpretation.
Any	The basic definition of each data value. Conceptually, it is abstract, which means that no value by itself can be a data value without belonging to a specific type.
Range	Set of ordered physical quantities, which indicate that the value comes from a possible range of values.
Range	The ranges for the upper and lower limits must be respected.
Range	No other options are allowed.
Range	The units for the upper and lower limits must match.
Range	Omitting or evaluating using exceptional values at the upper and lower limits is allowed.
Quantity	A dimensioned quantity expressed by the result to be measured.
Quantity	The unit must follow the recommendations in ISO 80000-1-2009; specifically, the International units system whenever possible.
Quantity	To communicate units between systems, we recommend the UCUM extensions. The UCUM must not be used in screen, visualization, or printing interfaces destined for human readership.
Period	A set of consecutive time marker values.
Period	Can be expressed using the start date and end date, start hour and end hour, or a range of time (for example, 3 months).
Period	A period must be represented specifying the start and end dates, and the start date and the width.
Period	No other options are allowed.
Period	A derived model can constrain the representation of a start and end date.
Period	Omitting or evaluating the used components using exceptional values is allowed.
Overall Time	Unordered number of different values which are amounts of time.

Specification	
Overall Time Specification	Abstract values which are used to specify a timeline for the events, in addition to the cyclical validity patterns which can exist for certain types of information.
Overall Time Specification	Any implementable specification must describe how this abstract pattern is achieved. This can be by combining intervals or related event times.
Overall Time Specification	No member of the set will be evaluated using null or exceptional values.
Chain	The text data mainly destined for automatic processing.
Chain	A chain must contain at least one character or have a null value.
Relationship	Can be used as a relationship to indicate, for example, the measurement of a drug's concentration.
Extensibility of the model	The derived model included in this document, including the implementable specifications, are allowed to constrain the model even further. This can be achieved by restricting an element's conformance force when explicitly allowed to, by compiling narrative descriptions within a single narrative block at a section level, by including additional elements in the existing sections, lists, and tagging concepts, or by adding non-IPS sections to the international patient Summary.
Extensibility of the model	Within the international patient summary, the recipient can securely back up the provision of healthcare even if the semantic of the extensions cannot be processed.

Functional Requirement Details – IPS – Patient Attributes

The attributes which provide data that can be used individually or collectively to identify or guarantee a person's identity to an attending physician at the place of care.

Requirement	Description
Name	The name can be formed by a sequence of parts of the given first name, last name, prefix, and suffix.
Name	It must be possible to provide representations of a single chain and based on the name components of a person in different scenarios, but they always need to reflect the jurisdictions and cultural practices.
Name	Preferential use of the name should be provided within borders. Cross-border environments should also be allowed.
Name	Unless otherwise specified, it should allow more name elements for the same person.
Name	It must include the given and family components, but at least one of them must be present in the name.
Name	In case of non-alphabetic representations of a name, at least one alphabetic representation must be provided.
Name	There must be more representations when the name is non-alphabetic.
Name	The options of "preferred name" or "alias" are implicit in the data type "Person Name".
Name	When more than one name component is provided, it must allow for distinguishing which one should be used.
Administrative Gender	Certain countries require an administrative gender as a part of the patient's identification, but it will not be used to record a person's sex.
Identification	The identification should be unique.
Identification	The insurance number must be used as an identifier if, and only if, required by the country of affiliation, because many countries require this number to finance healthcare should it be needed.
Address	The format of the addresses can vary depending on the countries.
Address	The address is required if known.
Address	If a known address is provided, it must include at least one part of the address.
Address	Never documented as a single chain.
Address	It may or may not include a unique code for specific purposes. If this attribute is not present, it is assumed that it is the predetermined address useful for any purpose.

Telecommunications	The phone number or email is required if known.
Telecommunications	At least one phone number or email must be provided.
Telecommunications	Both can be provided.

Functional Requirement Details – IPS – Healthcare Provider Attributes

The attributes related to patient contact and healthcare organizations relevant to the patient in relation to their IPS.

Requirement	Description
General	This attribute must contain a contact for the person, as well as the medical organizations relevant to the person.
General	The personnel working within a healthcare organization considered to be a provider can include both professionals and individuals who participate in healthcare activities.
General	The organizations which are responsible for financing, paying, or reimbursing healthcare are NOT considered healthcare providers. They are Healthcare Third Parties.

Functional Requirement Details – IPS – Patient Address List Attribute

This attribute provides the IPS with the address details for individuals and organizations relevant to the patient.

Requirement	Description
General	The address book is also known as the Contact Information, but it only the “Address Book” name must be used.
General	The information must reflect the current status. It should not include any historical data, such as former addresses.
General	In the case of Unplanned care, the data set as “preferred” corresponds to the minimum and concise contact details that were exchanged.
Organization	The preferred Healthcare provider is required if known.
Organization	The term “preferred” within the patient summary indicates that it is the most relevant entity to contact.
Organization	It might happen that there are individuals or organizations which can be contacted but aren’t present in the address book. If they are present, however, they must be assigned a specific role.
Organization	Even though the attributes are gathered under the same IPS component for convenience, it is not necessary for any implementation to handle them equally.
Person	The recorded patient address can be used as a way to identify the patient, as well as the country of origin and residency.

Functional Requirement Details – IPS – Advanced Directives Attribute

The advanced directives refer to when unplanned healthcare activities where an event is life-threatening and the patient or legal guardian has included stipulations of what should happen to the patient if the patient cannot make their own decisions.

Requirement	Description
General	All information related to the addresses of the individuals making the decisions must be found in the patient address book section of the IPS.
General	All legal matters and interpretation issues related to the recording and application of advanced directives will be approached in any implementation of the IPS.
General	If multiple advance directives exist, they will be displayed as a list.
General	A reference to a document (living will) can exist instead of free text, but this reference can be a URL that is not restricted to being referred to in that way.
General	The indicated or referred advanced directives must be up to date, and the clinical personnel providing healthcare must verify the validity of the data.
Confidentiality	This component can transfer confidential data beyond the data related to healthcare. If this section of the IPS refers to a legal document, there might be further required considerations.

Functional Requirement Details – IPS – Allergies and Intolerances Attribute

The information related to the treatment and provision of healthcare of a medical attending to identify problems or avoid adverse effects which can occur because of the care that is being provided. It is for this reason that any allergies and active adverse reactions must be listed in addition to any relevant history.

Requirement	Description
General	A section required within the IPS; it must be documented.
General	The absence, known and unknown, must be explicitly indicated.
General	If content exists regarding allergies or intolerances, the field must not be empty and the state of the content must be omitted, it is not mandatory.
General	If there are no allergies or intolerances, the lists must be omitted.
General	For cases in which allergies and intolerances are empty, there must be a statement explaining the absence of the data.
General	For cases in which the clinical status related to an allergy or intolerance is resolved, the end date must be specified.
General	The date of the allergy or intolerance must be provided with as much precision as possible.
States	The status of an allergy or intolerance must be indicated. For example, inactive, active, resolved, in remission, among others.
States	For cases in which the corresponding status is inactive, an exception can be generated to indicate the inconsistency.
Criticality / Severity	Each one of the allergies or intolerances must indicate the criticality/severity that they present to the patient.
Criticality / Severity	The criticality/severity will be assigned a value. For example, high or low risk to the patient.
Criticality / Severity	It might happen that there is a value that does not allow for an evaluation of the risk. In that case, it is assigned the value “Exception”.
Certainty	The statement about the certainty associated with the propensity of predisposition to become sick, or the potential reaction risk to the identified substance.
Certainty	The certainty must include the following values: unconfirmed, temporary, confirmed differential, refuted.

Certainty	Each one of the certainty states must be accompanied with the necessary clinical evidence and the diagnosis.
Propensity/Predisposition	The type of allergy and intolerance will be coded into three types: allergies, intolerances, and adverse reaction propensity.
Diagnosis	A code which indicates the type of reaction and the agent.
Diagnosis	A description with textual information will be allowed if the coded data is not available.
Reaction	A tag which recognizes other data related to a reaction.
Signs of the reaction	The clinical manifestation of the reaction. It can be included as a textual description when no coded data is available.
Severity	The coded element which describes the subjective evaluation of the severity of the condition.
Severity	The severity of the reaction must include a set of values which correspond to Severe, Moderate or Mild.
Agent Code	Related to when a specific allergen presents a predisposition toward an allergic reaction. To this end, it will be taken from a list of agents and codes associated with a set of values.
Category	The category of the allergic substance. It can have values such as Food, Medication, Environment, Biological.

Functional Requirement Details – IPS – Functional Status Attribute

The capacity of an individual to perform the normal activities required to satisfy their basic needs and the usual functions while still maintaining their own health and well-being.

Requirement	Description
General	A functional evaluation or a list of disabilities, or both, must be provided.
General	Each functional evaluation entry must include a result or a subordinated functional evaluation entry.
General	The subordinated functional evaluation does not need to include results.
Disability	An individual's disability must be identified with a code.

Functional Requirement Details – IPS – History of preexisting health conditions Attribute

A description of problems and diseases. It offers a historical context which allows for the patient's current health status to be viewed.

Requirement	Description
General	List of narrative and structured code.
General	List which only includes closed, resolved, or inactive problems.
General	Must allow for filters to be applied per time period or size restrictions.
Issue	Must contain states, at least active or inactive.
Resolved/Date	If the resolved issue contains a date, it must be included.

Functional Requirement Details – IPS – Pregnancy History Attribute

The current status of a woman in relation to an ongoing pregnancy. Provides all chronological information regarding any previous pregnancies if applicable.

Requirement	Description
General	In case of pregnancy, the probable delivery date must be included.
General	The date must include a month/year estimation, but no day element.
General	The information related to the pregnancy must be written in plain text or structured, but not in both.
General	The pregnancy history must be recorded in four manners: text, list of dates, results, or metrics.
General	One manner must be used, but this does not exclude the use of other summary descriptions for the exchange.
General	The necessary data related to previous pregnancies must be provided if they are known.
General	The same previous pregnancy dates might exist multiple times if there were multiple pregnancies.

Functional Requirement Details – IPS – Procedure History Attribute

A list of procedures the patient has undergone.

Requirement	Description
General	If the patient has undergone any procedures, the list must not be empty.
General	If the patient did not undergo any procedures, the list of procedures must be omitted.
General	Every procedure that was performed must include the date in which the procedure was performed.
General	Every procedure the patient has undergone will include a real description of the procedure. For example, surgical procedure and real description corresponding to an Appendectomy.
General	Optionally, it might be necessary to indicate the part of the body for which the procedure was performed.

Functional Requirement Details – IPS – Vaccinations Attribute

This item intends to list the vaccines administered to the patient, allowing the inclusion of COVID-19 vaccines if necessary. For cases in which there was an adverse reaction to a vaccine, it must be listed in the “Allergies” attribute.

Requirements	Description
General	If the person was administered any vaccines, the field must NOT be empty.
General	The field might be empty because there is no information available for the vaccine.
General	All vaccines administered to the patient must be included.
Vaccine	It must be possible to enter the type of vaccine for a specific disease or diseases against which the patient was immunized.
Vaccine	The administered medication, batch number and product code can be included for the administered vaccine. Alternatively, if only the brand name is known, it can be included.
Vaccine	The administration route for the vaccine must be recorded.
Provider	The healthcare provider responsible for the administration can be included as well as their contact information in case it becomes necessary.

Functional Requirement Details – IPS – Medical Devices Attribute

This item will list all of the implanted internal or external medical devices a patient has or might need in case of any planned interventions or necessary patient healthcare treatments.

Requirement	Description
General	If the patient has no implanted devices, the field must be omitted.
General	If the patient has any implanted medical devices, they must be stated. Pacemakers, defibrillators, implants, prosthetics, ferromagnetic bone implants are just some devices of paramount importance when providing healthcare and are of interest to the physician.
General	Each device must have a similar structure, type, identifier, and use date.
General	Regarding the date in which the device was first implanted, it is allowed to only display the placement year.
General	For any cases in which the patient had an implanted device and no longer has it, the date on which the device was no longer used must be specified. It is allowed to only display the end year.

Functional Requirement Details – IPS – Medication Summary Attribute

This item lists all of the medication relevant to the patient's healthcare status. The scope of this document is for the medication the patient is currently taking, whether they have been prescribed or not.

Requirement	Description
General	For cases in which the patient is not taking any medications, the reason why there is no data regarding medication must be specified.
General	The reason why the medication was prescribed must be included.
Medication	The product code is the most generic one to identify the product.
Medication	The common name for a pharmaceutical product can include the concentration of a drug. The name will be associated with the PhP ID L2 IDMP identifier if it exists.
Medication	Upon recommendation of the WHO, it is recommended to use the international common name, if it exists, or the common name recommended by the jurisdiction.
Medication	The administration route can be added.
Medication	The start and end date of the medication administration can be indicated for the treatments that require it. For the cases in which the administration of the medication is unlimited because it relates to an ongoing therapy, the end date will be taken as an exceptional value.
Medication	The medication dosage can be added.
Medication	The frequency of administration for the medication can be added, which can be per hour, day, week or month.

Functional Requirement Details – IPS – Healthcare Plan Attribute

This item must be complemented with a description of the healthcare expectations, which must include proposal, goals, or medical demands for monitoring, tracking, or improvement of a patient's condition. It will also include recommendations for the patient's healthcare but does not include medications.
It also includes the discharge plan, which relates to the document in which the patient's condition upon being released from the hospital is described with the goal of educating the patient about reducing risks for patients.

Requirement	Description
General	The plan must be written as a text or in a structured manner which makes it possible to enumerate multiple plans instead of a single, consolidated plan.
General	The plan must contain basic recommendations, references of an extended plan, or both.
General	Any past healthcare plans will not be required by the IPS.
Discharge Plan	Any planned observations, planned procedures, meeting, or immunizations can be included.
Discharge Plan	The discharge plan must be written in a single, narrative block.
Recommendation	A reusable structure for a healthcare plan.
Recommendation	Each one of the recommendations must include two dates if they are available.
Recommendation	A recommended treatment plan is required.
Recommendation	The plans must be retrospective, but the dates can be in the future.
Extended Plan	The extended plan is conditional and can be an alternative to the recommendations included in a treatment plan.

Functional Requirement Details – IPS – Problems Attribute

After reading the description of the Problems, you should have an overall perspective of the patient's healthcare condition. It can also describe any identified medical alerts or clinical risks which might be important when providing healthcare to a patient.

Requirement	Description
General	The list of problems must not be empty.
General	For cases in which there are no patient problems, a clarification must be added to indicate the lack of data.
General	A list of structured problems. The problem will be obtained from a set of values coded with a narrative description.
General	Only active or current patient problems must be listed.
General	The problems can be categorized as active, current, or unresolved.
General	A resolved problem can be included if it a cause of concern and should be monitored.
General	The problem's start date must be indicated.
General	If information exists regarding the healthcare provider or specialist contact, it can be added.

Functional Requirement Details – IPS – Results Attribute

This item gathers the results relevant to the patient's healthcare situation.
It may include laboratory results, pathological anatomies, and x-rays. It might be necessary to also include the source of the results and any audits.

Requirement	Description
General	Each one of the results must include a subordinated observation value.
General	In case of a subordinated observation, there must be a value.
General	The results correspond to a list which must include descriptions, dates, and data regarding the source.
General	It will be possible to identify who made the observation. For some results, the roles of the executioner and the observer might coincide.

Functional Requirement Details – IPS – Social History Attribute

The social history of the patient refers to the social factors which can be considered as being relevant, such as alcohol consumption or tobacco use, since they are considered to be lifestyles which pose a risk to the patient.

Requirement	Description
General	The information must always appear in the IPS if it is available.
General	No exceptions have been raised for when the information is not available.
General	In case of any entries, they must be structured and coded.
General	The description of the lifestyle can be written in a narrative form.
General	Any observations related to the different lifestyles.
General	The lifestyle observations may cover a period of time. The dates must at least include the years.
General	Depending on the jurisdiction, the lifestyle factors might correspond to sensitive information which requires special confidentiality rules.

Functional Requirement Details – IPS – Vital Signs Attribute

This item indicates any relevant results coming from the recording of the patient's vital signs. In addition, it might include data such as the height, weight, and BMI.

Requirement	Description
General	Each one of the vital signs must include a value or a subordinate vital sign, but never both.
General	Any subordinate vital signs must include a value.
General	It might be possible that the observation does not have any vital signs relevant to the patient's present.
General	The types of results must include a date, source, and description.
General	The common types of vital signs correspond to Temperature, Blood Pressure, Cranial Perimeter, Heart Rate, Heigh, Oximetry, Weight, BMI.

Functional Requirement Details – IPS – Cross-Border Attribute

The data included in this item are necessary for cross-border transactions.

Requirement	Description
General	They are only mandatory for cross-border applications.
General	They must contain information regarding the corresponding country of affiliation for the patient, in addition to healthcare information.
General	It might be possible that a specific country requirement is needed corresponding to a description of a one-off occurrence. This must be declared as part of the cross-border information. It might include a consent.

Functional Requirement Details – IPS – Source Metadata Attribute

We refer to the source Metadata to offer context of the information that is being provided, which increases confidence in the data that will be exchanged.
Any information regarding the source of the data is necessary to identify who the summary belongs to.
It is important to mention that there are three approaches to create a summary:

- Direct human intervention from a healthcare actor.
- An automatic approach.
- A mixed approach.

Requirement	Description
General	The source of the information is usually the patient.
General	The IPS document can be created only once, but it might include different dates as a consequence of any updates made to the information it contains.
General	For the origin to be verified, at least one organization must be included as the author of the document. If there is no information related to a healthcare professional, the healthcare organization must be featured.
General	The responsible healthcare professional or provider must attest or sign the patient's information depending on the jurisdiction.

Non-Functional Requirements

Basic Concepts

The quality attributes which are expected from the system. They are the conditions under which any digital system must remain effective.

Non-Functional Requirement Details

Following are some important concepts related to these non-functional requirements which correspond to the ones detailed by the WHO[11].

- Accessibility: it must adapt to the needs of the users who will be accessing the system, and it must contemplate users with disabilities.
- Availability: the time during which the system will be available.
- Capacity: the number of users that will be using the system simultaneously, in addition to the system's performance and its response capacity.
- Activity time: refers to the recovery time for critical or unexpected failures, and the system's redundancy to minimize any losses of data.
- Performance / response times: the speed with which the system responds.
- Platform compatibility: refers to all the operating systems, machines, and configurations in which the solution is expected to be executed.
- Security and privacy: the security levels in terms of user authentication and data protection.
- Regulation and compliance: all legal restrictions that the system must comply with.
- Reliability: a measure of the tool's reliability.
- Scalability: the capacity and strategy to improve the increasing load of the solution. The solution can be scalable horizontally (if more elements are added to the solution) or vertically (if capacity is added to the existing elements).
- Supportability: the requirements to detect, diagnose, resolve, and supervise any system failures. It relates to the technical support.
- Usability: the efficacy, efficiency, and user satisfaction.
- Retention/data archiving: the mechanisms used to archive the solution.

Requirement	Description
Accessibility	Optimizing the delivery of information to users in areas of poor connectivity.
Accessibility	The solution must be available offline.
Accessibility	It must provide a resynchronization mechanism to send the data that was created offline when the solution is back online.

[11] Digital Documentation of COVID-19 Certificates. Testing Results – Technical Specifications and Implementation Guidance. WHO – November, 2021.

Accessibility	The solutions must follow best practices to offer clear, intuitive, and coherent interfaces so that different users with cultural differences can still access the system.
Accessibility	Optimizing the interface so it can be adapted to any device.
Availability	The developed solutions must not have more than 10-minute interruptions, and no more than 1 minute worth of data loss or response will be accepted.
Availability	There must be an indicator of the solution's availability so users can verify the system's status.
Capacity (current and predicted)	A potentially large number of simultaneous users must be able to access the system and perform reading and writing transaction during the normal operation.
Capacity (current and predicted)	At peak times, the system must increase the user traffic.
Capacity (current and predicted)	Anticipate that the user base growth will be high. As a security measure, the system should prepare, or have scalability plans to prepare, for a 5% annual increase.
Disaster recovery/resilience	The data and derived analysis must be stored within a data architecture which guarantees redundancy and a quick recovery of the data to discard any potential losses.
Disaster recovery/resilience	The system should be able to provide almost instantaneous changes in case any architecture components experience a critical failure.
Disaster recovery/resilience	Provide an almost instantaneous switch in case of any physical failures of an architecture component.
Disaster recovery/resilience	All of the solution's components must have backups.
Disaster recovery/resilience	The system data will be available to all system administrators, who can use a dashboard to display the current and recent load, in addition to any custom queries by location and time.
Disaster recovery/resilience	Automatically record any system interruption periods, complement, and update this record manually.
Disaster recovery/resilience	Activate system alerts depending on the activity time and performance.
Disaster recovery/resilience	Use alerts to perform actions such as sending emails and messages.
Performance/response times	The solution must follow best practices to offer a receptive interface which can handle the typical requests within a maximum amount of time defined in seconds which will be determined by the typical bandwidths.

Performance/response times	It must have a design which minimizes any performance degradations as a consequence of load increases.
Performance/response times	For processes with long executions, such as complex queries, the system must be available for asynchronous executions so that users can continue to interact with the system while the work is executed. A notification will be received when the work has been completed.
Performance/response times	Implement a detection mechanism for frozen interfaces (“hung”) to give the users the option to cancel the current request.
Performance/response times	The system must be able to obtain performance metrics and response times which make it possible to identify problems to proactively address any types of risks.
Performance/response times	Allow queries to be ran regarding performance records and to export performance data to be used in reports.
Performance/response times	It must be possible to set a performance threshold and to generate any necessary alerts in case those thresholds are not met.
Security/Privacy	The necessary tools to request a new account, to log in, to close the session, so set and change passwords, and to receive password reminders must be provided.
Security/Privacy	Any interactions between the component and the clients must be encrypted.
Security/Privacy	Any cloud component of the solution must store idle cloud data with an encrypted format. It must contain a robust and flexible security model, control access to the data such as the operations that can be done with the data.
Security/Privacy	Any information provided on the governance and use of data must be available with a special emphasis on the level of confidentiality and sensibility.
Security/Privacy	Panels, reports, standard queries, and information exports must be provided to help system administrators manage access permissions.
Security/Privacy	Careful handling of data confidentiality.
Regulation/Compliance	The architecture’s design must take into account reference guidelines and standards.
Regulation/Compliance	There must be a compliance with data policies and legal requisites identified by the jurisdiction of the country in which the solution will operate.
Regulation/Compliance	The data set must be tagged with any regulation and compliance information that is relevant to them so that it is easily available with the data set.

Regulation/Compliance	Comply with any storage, retention and data destruction laws required by data policies and data laws from the countries in which the data is stored.
Reliability	There must be a design which minimizes the average time between failures, and which offers best practices for a slid, proven, and reliable platform.
Reliability	Generate a record of the failures produced anywhere within the system, which will allow calculations and tracking of the average time between failures.
Scalability	The design must allow for both the elements and the mechanisms to scale horizontally in order to coordinate their activities.
Scalability	The design must allow for the elements to scale vertically.
Scalability	Configuration of automatic horizontal scaling rules which allow for the system to respond to load increases. The rules must be based on load thresholds and the system's performance.
Scalability	Record as much information as possible regarding the system's performance and load times to refine the scalability strategies to scale the system based on its real use.
Compatibility	Record the system's activity so that events of interest can be recorded with the time and date at which they occurred, their category, and the user (if applicable) who triggered the event. The record must have as many details as needed to help the technical support personnel debug any problems.
Compatibility	For recording purposes, use a detailed and standard format. For the details, use the trial or error adjustment periods. For the standard format, use the system in production.
Compatibility	The technical support personnel can filter and run queries to check the system records and quickly identify any areas of interest.
Compatibility	Activate alerts related to the creation of predefined recording entries.
Compatibility	Have a published strategy for any patch releases, maintenance releases, and version updates.
Usability	Consider the best practices for user design / adaptative design to guarantee the best chance of creating a clear, concise, and intuitive user experience. This is particularly relevant for any interface handling data entries.
Usability	Navigation must be possible using only the keyboard.
Usability	The solution must be adaptable to any device.
Usability	Provide an easy way to manage the taxonomy to record

	standard definitions, relationships between terms, etc.
Data Retention/Archiving	Manually request an archive from a selected subset of information.
Data Retention/Archiving	Program the archive from a selected subset of information and set a repetition for this operation. The archiving operation will execute when the programmed date and times come.
Data Retention/Archiving	Activate a notification alert when an archiving operation is completed including any success or error reports.
Data Retention/Archiving	No archiving function will affect the system's performance.
Data Retention/Archiving	Any archive material must be tagged with metadata about the information it contains, and the date and time when it was created, to make it easier to quickly navigate through all of the archived material.
Data Retention/Archiving	All archive operations must be recorded.
Data Retention/Archiving	If users have the necessary permissions, they should be able to perform a limited query of the archive contents to identify any information of interest.
Data Retention/Archiving	If users have the necessary permissions, they must be able to restore the information contained in a selected archive.
Data Retention/Archiving	All of the information within an archive must be encrypted to avoid any unlawful sues if the system is accessed by an unauthorized person.

The definition of the Functional and Non-Functional requirements will allow for a correct exchange of information regarding the any Vaccination Certificates between countries in Latin America and the Carribbean.

Glossary

CTR	Regional Technical Committees
PoCs	Proofs of Concept
DGC	Digital Green Certificate
EU	European Union
EHN	European Health Network
EUDCC	EU Digital Covid Certificate
HSM	Hardware security module
DGCG	Digital Green Certificate Gateway
1D	Unidirectional
2D	Bidirectional
DDCC	Digital documentation of COVID-19 certificates
DDCC:VS	Digital documentation of COVID-19 certificates: vaccination status
HICD	Healthcare Certificate Identifier
ID	Identifier
PHA	Public Health Agency
NAAT Test	Nucleic acid amplification test (NAAT), such as polymerase chain reaction with reverse transcription (PCR-RT), loop mediated isothermal amplification (LMAP), or transcription-mediated assay (TMA) to detect the presence of ribonucleic acid ARN for SARS-CoV-2.
Rapid antigen test (RAT)	Test based on the detection of virus particles (antigens) via a lateral-flow immunoassays which provides results in less than 30 minutes.
Antibody testing	Laboratory test meant to detect if a person has developed antibodies for SARS-Cov-2, which indicates that the certificate owner has been exposed to SARS-Cov-2 and has developed antibodies, regardless of whether the person was symptomatic or not.
IHE	Integrating the Healthcare Enterprise
EHR	Electronic Health Record
IPS	International Patient Summary

BMI	Body Mass Index

Bibliography

- WHO- Digital Documentation of COVID-19 Certificates. Vaccination Status – Technical Specifications and Implementation Guidance. August, 2021
- eHealth Network – Verifiable Vaccination Certificates – Basic interoperability elements. Version 2 – 2021-03-12
- eHealth Network – Technical Specifications for EU Digital COVID Certificates – JSON Schema Specification – Version 1.3.0 – 2021-06-09
- Digital Documentation of COVID-19 Certificates. Testing Results – Technical Specifications and Implementation Guidance. WHO – November, 2021
- eHealth Network – Value sets for EU for the Digital Green Certificate. Version 1.0 – 2021-04-21
- REGULATION (EU) 2021/953 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 14 June 2021
- ISO 27269:2021(E) – Health Informatics – International Patient Summary – First Edition 2021-04
- https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_es
- https://www.hl7.org/fhir/profilelist.html
- http://hl7.org/fhir/documentreference.html