Issuance of Digital Covid Certificates (Vaccination & Recovery)

Data Protection Impact Assessment

Version 0.7

Rialtas na hÉireann
Government of Ireland

An Roinn Sláinte
Department of Health

Seirbhís Sláinte Níos Fearr á Forbairt | Building a Better Health Service

Table of Contents

Version History

Version	Date	Description
0.1	8/07/2021	First draft development.
0.2	11/07/2021	Second Draft following feedback from Peter Lennon and Muiris O'Connor.
0.3	14/07/2021	Third Draft following feedback from Peter Connolly, Chris Meehan, Orlaith McGee and Jim O'Sullivan.
0.4	19/07/2021	Fourth Draft following feedback from Peter Lennon and Mary Saunderson.
0.5	20/07/2021	Fifth Draft following additional feedback from Jim O'Sullivan, Peter Lennon and Peter Connolly.
0.6	28/07/2021	Sixth Draft incorporating DoH and HSE DPO comments.
0.7	15/11/2022	Seventh draft reflecting transition of DCC service desk operations from Accenture (3rd party provider) to HSE Live (internal provider with access to Covax, IIS and HSE data resolver teams)

Digital Covid Certificate - Context

The EU Regulation on Digital Covid Certificates[1] provides for and requires Member States to issue Digital Covid Certificates to those entitled to receive them and provides the legal basis for the necessary processing -Article 6(1)(c) GDPR (compliance with a legal obligation) and Article 9(2)(g) GDPR (substantial public interest).

The overarching objective of this Digital Covid Certificate as set out in the EU Regulation is:

"…to facilitate the application of the principles of proportionality and non-discrimination with regard to restrictions to free movement during the COVID-19 pandemic, while pursuing a high level of public health protection"

The Department of Health (DoH) and Health Service Executive (HSE) are engaged together with regard to the generation and delivery of the Digital Covid Certificate in Ireland (DCC) for both vaccination and recovery streams. This Data Protection Impact Assessment (DPIA) sets out details of the key actors involved in the generation and dissemination of the DCC, the systems used and the information that these systems require in order to ensure that the Digital Covid Certificate delivers on its purpose and is received effectively by the wider public.

As the name indicates, the focus of the DPIA is on the data protection (privacy) aspects of the DCC generation and dissemination but it also has the broader goal of helping to ensure public confidence in the programme.

The aim of the DCC programme is to facilitate free travel amongst the EU Member States and reduce undue burden on EU citizens and national border control resulting from unviable/fraudulent means of verifying an individual has been appropriately vaccinated against/recovered from Covid-19. This verification is critical as it assists in further mitigating disease at the population level.

In line with the streams detailed below, the Department of Health and Health Service Executive will issue either a digital or physical DCC to all relevant members of the public. The initial rollout of vaccination certificates will be conducted as a matter of wider public interest and, as such, is not subject to opt-in.

The national Digital Covid Certificate programme can only work both for individuals and society if it is supported by information systems capable of capturing and processing relevant and necessary information. Where that relevant and necessary information is personal data (that is information about a living, identifiable individual) it falls under the EU General Data Protection Regulation (GDPR).

The purpose of this document is to transparently assess the impact of the envisaged operations on the protection of personal data and how the rights to privacy and confidentiality of the users are appropriately protected. In line with the scale of the required data processing and categories of data processed, the carrying out of this assessment is considered appropriate and desirable.

As the DCC programme continues to evolve there are likely to be changes to the DCC distribution strategy, the associated processes and operating model and the underlying technology solutions, this DPIA should be viewed as a living document that will be updated as necessary to ensure that its contentsalways reflect any material change.

[1] REGULATION (EU) 2021/953 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.

1. Overview

Regardless of whether a physical or digital DCC is generated, the underlying approach and process will be similar. The DoH and HSE, acting as joint data controllers are developing an end-to-end, comprehensive solution to underpin this process and support the delivery of the Digital Covid Certificate.

Under the GDPR, processing of personal health data is generally prohibited, unless it falls into one of the expressly foreseen scenarios in Articles 6 and 9 of the GDPR (i.e. there is a 'lawful basis'). The processing of personal health data (to the extent that it is necessary and proportionate) from the HSE Vaccine Information System (CoVax) and HSE CovidCare Tracker (CCT) System is required for the purpose of generating and disseminating the DCC to enable the free travel of individual citizens and the public generally. The impact of the operation of issuing the DCC on the protection of personal data and how the rights to privacy and confidentiality of users are protected will be formally assessed as part of this Data Protection Impact Assessment.

It should be noted that the EU Regulation recognises that Member States may choose to use the Digital Covid Certificate for purposes other than travel. As such other uses would, under the EU Regulation, require a separate and distinct legislative framework to underpin those uses and involve consultations with the Data Protection Commission they are outside the scope of this DPIA which is concerned with the issuing and verification of the Digital Covid Certificates for vaccination and recovery.

2. Scope

The EU Digital Covid Certificate Regulation provides that individuals may receive a digital covid certificate through one of three streams:

1. **Vaccination**
2. **Recovery**
3. **Test**

However, while three streams are encapsulated within the wider Digital Covid Certificate programme, the Department of Health and HSE, as joint data controllers, have been specifically tasked with the generation and distribution of the Vaccination and Recovery DCC streams only.

The Testing stream will be operated and run by private labs who act as independent data controllers in their own right. In terms of test certificate generation and distribution, the overall process will be similar to the vaccine and recovery streams, with OGCIO still acting as a data processor to the private lab in question. Individuals seeking a Test Certificate should engage directly with the lab carrying out the test.

To that effect, this DPIA will only consider generation and issuance of the Digital Covid Certificate for Vaccination and Recovery streams.

2.1 Vaccination Certificate:

The vaccination stream of the Digital Covid Certificate will be used to verify the current vaccination status of a given individual. The underlying data required to generate and issue the certificate has been extracted from the HSE Covax system via the HSE IIS data lake which, provided the given individual has been fully vaccinated, contains all material data required to fulfil this purpose.

The vaccination certificate will be issued to applicable individuals free of charge via email or post.

2.2 Recovery Certificate:

The recovery version of the Digital Covid Certificate will be used to verify whether a given individual has contracted a strain of Covid 19 and their subsequent recovery[2] from same. The underlying data required to generate and issue the certificate has been extracted from the HSE CCT system via the IIS data lake and contains all material data required to fulfil this purpose.

[2] Patients/data subjects are deemed eligible to receive the Recovery DCC eleven days following receipt of a positive NAAT test.

Unlike the vaccination certificate, individuals will need to request their recovery certificate and this will be managed through the DCC call centre (further described within section 3.3 below)

The recovery certificate, once generated and requested via the DCC call centre, will be issued to applicable individuals free of charge via email or post.

2.3 Data Controllers & Data Processors:

The diagram below shows the logical flow of data between the DoH/HSE and the various other stakeholders who will participate in the end-to-end process.

Figure 1 – Data Controller/Processor Flow Chart

The table below summarises the roles of all key parties who will provide data or have access to data processed for the purpose of the Digital Covid Certificate scheme. Contracts are in place between the Department of Health, HSE, Department of Public Expenditure and Reform and each of their associated ancillary parties which set out the processors' obligations and the Department of Health/HSE's obligations and rights with regard to the personal data that is being processed.

These contracts comply with the legal requirements for joint data controller and data processor contracts set out in the GDPR under Article 26 and Article 28 respectively. All third-party access to personal data shall be managed in accordance with the relevant IT security policies. The level of access and the access privileges will be agreed with the third party on a case by case basis.

Data Map Ref	Members	Data Role	Role Summary
1	**DoH**	Joint Data Controller	The Department of Health acts as a Joint Data Controller alongside the HSE for the purpose of generating and issuing the DCC for both vaccination and recovery streams. The Department of Health does not hold any personal data relating to generating and issuing the certificates.
2	**HSE**	Joint Data Controller	The Health Service Executive acts as a Joint Data Controller alongside the DoH for the purpose of generating and issuing the DCC for both vaccination and recovery streams. The role of the HSE is the provisioning of data for the purposes of the issuing and verification of vaccination certificates and recovery certificates. The HSE Live team is responsible for managing the call centre helpdesk established to assist members of the public with DCC related queries. This will include requests for amendment and acting as contact point for requesting a recovery DCC.
3	**Microsoft**	Data Processor	Microsoft are a cloud service provider for the HSE. Microsoft also provide the Dynamics CRM on which the CovidCare Tracker (CCT) system is hosted.
4	**IBM**	Data Processor	Data Processor responsible for configuring and implementing the Vaccine Information System (CoVax) on behalf of the HSE.
5	**Salesforce**	Data Sub-Processor	Data sub processor for the Vaccine Information system working in conjunction with IBM to implement and host the system (and data).

6	**EY**	Data Processor	EY provide professional services in Data Architecture, Data Platform, Data Engineering, and Data Analytics to the HSE to support the HSE's Integration Information Services (IIS) Datalake. The IIS Datalake is a data aggregation platform in the HSE which brings together key data sources for managing the COVID pandemic such as Lab Results, Test and Trace cases, and Vaccinations.
7	**Amazon**	Data Sub-Processor	Amazon will act as a data sub-processor to HSE Live in providing a telephony service via Amazon Web Services Connect Cloud.
8	**DPER (OGCIO)**	Data Processor	The Department of Public Expenditure and Reform and, more specifically, the Office of the Government Chief Information Officer will act as a data processor for the DoH/HSE and has been tasked with the generation and distribution of the DCC in both digital and physical formats.
9	**NearForm**	Data Sub-Processor	Nearform, while acting as a data sub-processor to DPER (OGCIO), develop and manage the API used to ensure that the JSON and Manifest files issued by the HSE are picked up and issued to the respective system for issuance. Nearform also act as the developer of the verifier app to be used by border control under the authority of the Department of Justice. However, this element falls outside the scope of this DPIA.
10	**Qryptal**	Data Sub-Processor	Qryptal, while acting as a data sub-processor to DPER (OGCIO), will generate the QR codes required for the DCC.
11	**Revenue**	Data Sub-Processor	The Department of Revenue, while acting as a data sub-processor to DPER (OGCIO), will be responsible for the mass printing and distribution of physical DCCs.
12	**Amazon**	Data Sub-Processor	Amazon Web Services are a cloud service provider for DPER (OGCIO). Amazon also provide a bulk emailing service allowing for the wider distribution of the DCC via that medium on behalf of the DoH/HSE.

3. Roles and Responsibilities

3.1 Issuance and Verification of the DCC (Vaccine & Recovery)

The DoH and HSE have been tasked with the issuing and verification of the vaccination and recovery Digital Covid Certificate.

For the purpose of issuing and delivering both vaccination and recovery certificates, the Department of Health has entered into a joint data controller arrangement (under Article 26 of the GDPR) with the Health Service Executive as both parties will jointly determine the purpose and means of the processing envisaged.

3.2 Data Collation

The HSE has been tasked with the collation of the necessary vaccination and recovery data in order to allow for the generation and delivery of the DCC. This data will be shared with the Department of Public Expenditure and Reform (OGCIO), acting as a data processor, to facilitate the generation and distribution of the DCC.

The personal data in question was previously captured via the HSE managed Covax and CCT systems. A high level overview of the processes involved is provided in appendix A.

CoVax: All vaccination data required to generate and issue the vaccination stream DCC is contained within the HSE CoVax system. The CoVax system in turn is a repository of vaccination data stemming from GPs, mass vaccination centres and pharmacies across the country. CoVax servers are hosted on the secure Salesforce Cloud and within Salesforce data centres within the European Economic Area.

CovidCare Tracker (CCT): All recovery data required to generate and issue the recovery stream DCC is contained within the CCT system. The CCT system in turn is a repository of patient data relating to initial assessment, Covid-19 testing, contact tracing and clinical management. The CCT system is hosted on a secure Microsoft Dynamics CRM and within Microsoft data centres located within the European Economic Area.

Data originating from the above systems is imported to the HSE IIS data lake[3] where it is then parsed to generate the specific underlying files required by the Department of Public Expenditure and Reform (OGCIO) for the DCC. A high level overview of the processes involved is provided in appendix A.

3.3 Generation and Distribution of the Digital Covid Certificate

The Department of Public Expenditure and Reform (OGCIO), while acting as a Data Processor, is responsible for generating and disseminating the Digital Covid Certificate and does so under the direct control and authority of the Department of Health and HSE acting as joint data controllers.

Having received the respective data via secure transfer, an application programming interface (API) will then create the DCC, incorporating a secure QR code, and begin batching the files into two respective streams for distribution:

Email distribution –
This will be actioned via Amazon mailshot directly by OGCIO, though the email will come from a No-Reply DoH email address.

Postal distribution –
OGCIO will group the respective batch of DCCs and present same to Revenue.
Revenue, while acting as a data sub-processor, will then draw down the certificates for printing and distribution via post.

Once a given batch of certificates has been distributed, a batch delivery report will be generated and issued to the DoH/HSE for verification purposes. Data is retained temporarily for troubleshooting and for audit and trace for all certificates issued. This is to ensure relying parties are acting in good faith, to protect the integrity of the certificates issued, and to support any investigative process.

A high level data flow chart outlining this process has been provided in appendix B.

In the event of failed delivery, the following processes are in place:

Email – Bounced emails will be highlighted via Amazon mailshot capability to OGCIO, who in turn will encompass this information within the delivery status report issued to the HSE each day. The HSE, will then provide this update to the DCC call centre.
Postal – Undelivered post will be returned to Revenue for processing.

3.4 Call Centre Support Service

The HSE contact centre, HSE Live will provide a call centre support service operated on behalf of the DoH/HSE which enables individuals to raise queries and issues regarding the DCC programme as well as well as request their own DCC insofar as the

[3] The HSE IIS data lake is a data repository wherein all information originally residing in CoVax, CCT and other HSE operated systems ultimately flows. This repository serves a number of critical functions, not least of which being the primary source of information for generation of both the vaccination and recovery DCC streams.

recovery stream is concerned. This call centre is reachable via a phone and complement digital channels/portals available to support online requests for DCCs.

The Department of Health and the Health Service Executive acting as joint data controllers will provide such personal data on vaccination and recovery from the CoVax and CovidCare Tracker systems (described above) to HSE Live as are necessary to provide a service to callers. More specifically, HSE Live will have limited access to vaccination and test data required to answer individual queries on the digital covid certificate and limited patient data required to process requests for recovery certificates.

Call centre agents will be in a position to create basic amendment requests for the Covax and CCT systems, which in turn will update the IIS data lake and allow for re-issuance of certificates in the event of:

- Email address being incorrect or not having been provided in the first instance
- Postal addresses being incorrect (where certificate is to be posted)
- The first name is incorrect (subject to inbuilt tolerances)
- Certificate details are correct, but the certificate has not been received via email or post

For more complex requests requiring additional verification, call centre attendants will escalate the request to the HSE resolver team. The resolver team will determine whether such requests are to be accepted and will be screened to ensure appropriate due diligence. Examples of such requests include:

- Any material change to data other than the fields outlined above (such as vaccination data, change to date of birth etc.)
- New certificate requests (Recovery)
- Any other instance wherein the call centre agent cannot find the certificate referred to

Where a request is accepted, certificates will be re-issued through existing processes and in line with the flow chart outlined in appendix D. Where a request is rejected, the HSE resolver team will update the DCC Call Centre who will then contact the individual requester to explain the rejection.

All complex queries and amendment requests will be issued via the HSE Salesforce Service Cloud facility.

4. Processing Overview

The Digital Covid Certificate establishes a standardised, multijurisdictional approach for admission to a given EU Member State.

The DCC service is live since 19th of July 2021and the service and will continue to be offered so long as it is people require EU digital covid certificates.

4.1 Necessity & Proportionality

The Digital Covid Certificate is both necessary and proportionate to:

- ✓ Ensure the rights of EU citizens to freely move and reside across the Member States
- ✓ Ensure a well-co-ordinated, predictable and transparent approach to restrictions on freedom of movement
- ✓ Reduce the risk of forgery and false certificates

The adoption of unilateral or uncoordinated measures regarding certification for vaccination and recovery from Covid 19 is likely to lead to restrictions on free movement that are inconsistent and fragmented, resulting in uncertainty for EU citizens when exercising their EU rights. To that end, dissemination of the DCC and similar implementations is crucial not only in Ireland, but across the European Union.

It is the view of the DoH and HSE that in order to effectively and efficiently manage the deployment of the DCC to the population, there is not a less intrusive methodology to undertake this task. In addition to establishing the principle of necessity and proportionality, the principle of data minimisation has been adopted throughout. This will limit the processing of personal data to the minimum necessary, by only including a limited set of personal data on the certificates to be issued.

4.2 EU Interoperability

The Digital Covid Certificate has been designed in line with EU guidelines which supports interoperability across all EU Member states.

5.Scope of Processing

This section of the document describes the data that will be processed, how much data is being collected and used, how often it will be processed, how long it will be retained for, and who the data relates to.

5.1 Data Subjects

The proposed data processing relates to all individuals in the Republic of Ireland that are administered the COVID-19 vaccination as well as those who have been recorded as recovered from Covid-19.

5.2 Data Types

Generation and issuance of the Digital Covid Certificate requires the processing of various categories of data. The table below lists the data types and provides a definition for each. Examples are also provided for each data type:

Data Type	Definition	Examples
Personal Data	Personal Data required to generate and issue the Digital Covid Certificate.	Forename, Surname, Date of Birth, Email, Home Address
Special Category Data	Special Category (Health) data required to generate the Digital Covid Certificate	Vaccination Status, Recovery Status
Vaccine Data	Non-personal information relevant to the vaccine being administered to the patient	Vaccine Name, Vaccine Brand, Vaccine Batch Number
Certificate Meta Data	Non-personal information required to distinguish between certificates	Universal Certificate Identifier, Certificate Issuer

5.3 Personal Data Collected/ Processed

The information processed during the generation and distribution of the digital covid certificate is a combination of personal data and special categories of personal data (health related data). Information is processed on various systems by multiple parties along the generation journey as seen in section 2. Existing data will be collated during the initial phase of the digital covid certificate generation process. This includes data residing in the Covax system and CCT systems respectively.

The data sets extracted for the purpose of the vaccination and recovery DCC streams leverage the minimum data set as prescribed withing Regulation (EU) 2021/953.

5.4 Data Retention

There are various retention limits on different types of data being processed for generation and issuance of the Digital Covid Certificate and these are outlined in the table below. The specific data sets extracted in order to generate and issue the DCC will be retained by the parties for no longer than strictly required and in any case, no later than the 30/6/2023.4

However, it should be noted that the underlying data sets residing in the CoVax and CCT systems respectively will be held in perpetuity by the HSE and fall outside the scope of the below table.

Data Type	Entity	Retention	Retention Justification	Retention Measure
Personal/Special Category Data – JSON/Manifest Files	HSE/DoH/DPER	The specific data sets used to generate the two certificate variations will be held for 72 hours.	The justification to store personal data for this period is to facilitate the availability of the data to those generating the certificate.	It is intended that data specifically extracted to generate the two digital covid certificate variations will be securely erased after 72 Hours.
Vaccine Data – JSON/Manifest Files	HSE/DoH/DPER	The specific data sets used to generate the two certificate variations will be held for 72 hours.	Vaccine data is non-personal data. The justification to store the data for the period indicated is to facilitate the availability of the data to those generating the certificate.	It is intended that vaccine data specifically utilised to generate the digital covid certificate will be securely erased after 72 hours.
Personal/Special Category Data - Call Recordings	HSE Live	Call recordings will be retained for 28 days.	The justification to store recordings for this period is to facilitate necessary operational/verification requirements.	It is intended that call recordings will be erased after 28 days.

5.5 Parties who will Access/Use Personal Data

The Department of Health and HSE shall enter into the appropriate agreements with all third parties who are provided with direct access to patient information and/or are provided with personal data from any supporting systems. These agreements will outline each parties' responsibilities and the scope, purpose, duration and means of processing undertaken by each party.

The table below details the level of access to the data that each of aforementioned groups will have.

Members	Data Role	Data Access
Department of Health	Joint Data Controller	- N/A

4 Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.

Health Service Executive	Joint Data Controller	- Patient Data
Department of Public Expenditure and Reform	Data Processor	- Limited Patient Data Required to Generate and Distribute the Digital Covid Certificate

5.6 Personal Data

This section describes how personal data will be collected, used, transferred and if necessary, kept up to date. The underlying vaccine information system (CoVax) and CovidCare Tracker system (CCT), via secure sign-in, and IT/network security standards already established, will allow secure updates by centralised teams. Updates to data will almost instantly enter the database and will be shareable with all teams requiring access to information for the purpose of generating and issuing the certificate.

The following scope for personal data processing has been determined. A rigorous data minimisation approach has been adopted to personal data processing and only personal data that is necessary and proportionate to generate and issue the Digital Covid Certificate will be processed in line with Regulation (EU) 2021/953.

The following table sets out the personal data that will be processed in order to generate and issue the Digital Covid Certificate. The table provides a description of the data, the source, the type of data and how often the data is processed.

Data *Data Points to be collected from within existing dataset*	Data Type *(Personal Data / Personal Health Data)*	Collection Activity *Event at which data was captured*	Collection Frequency *Frequency at which data will be captured*
First Name	**Personal Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.
Surname	**Personal Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.
Date of Birth	**Personal Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.
Email	**Personal Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.
Home Address	**Personal Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.
County	**Personal Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.

Country	**Personal Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.
Eircode	**Personal Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.
Vaccination Status	**Personal Health Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.
Disease or Agent Recovered From	**Personal Health Data**	Extracted from Covax/CCT	Collected as required in order to generate and issue a valid digital covid certificate.

6. Context of Processing

Under the GDPR, processing of personal health data is permitted subject to there being a valid lawful basis for the processing in Article 6 (Lawfulness of processing) and Article 9 (Processing of special categories of personal data) of the GDPR (The lawful basis for the processing of the personal data as part of the Digital Covid Certificate programme is discussed in section 8). Processing must also be in accordance with the data protection principles set out in Article 5 (Principles relating to the processing of personal data).

The processing of personal and special category health data for the purpose of generating and issuing the Digital Covid Certificate is required to ensure, to the maximum extent possible, the freedom of movement for members of the public.

6.1 Children

Children aged 16-17 with underlying conditions that place them at very high risk of serious disease should they contract Covid-19 have been vaccinated. While members of this cohort have been vaccinated and their personal data has been captured as part of the vaccine administration process, this cohort will not be immediately eligible to receive the Digital Covid Certificate.

As the Digital Covid Certificate will not be issued to under 18s at this moment in time, it is therefore not considered under review for the purpose of this DPIA.

7. Stakeholder Engagement

Stakeholder engagement has been conducted to support and inform the development and deployment of the Digital Covid Certificate as part of the ongoing project. The purpose of these consultations is to ensure that all processing activities encompassed within the wider programme are configured to reflect the clinical, operational, and reporting requirements that underpin the Digital Covid Certificate.

From a development perspective, the following considerations were addressed: system functionality, appropriate use of data, information security, accessibility.

Due to the time constraints regarding the dissemination of the Digital Covid Certificate, a consultation process was not conducted with the public.

8. Compliance with Data Protection Law and other Regulatory Guidance

The following sets out the lawful basis for the processing of personal data identified in Section 5 of this document. The processing activity is included in brief for convenience.

8.1 Lawful basis for further processing of pre-existing personal data – Vaccination/ Recovery Stream

The generation and issuance of Digital Covid Certificate to individuals will involve the processing of pre-existing personal and special categories of data. While individuals must provide their consent to receive the Covid-19 vaccine, this consent is in the form of 'medical consent'. Consent as outlined under Articles 6 and 9 of the GDPR is not used as a lawful basis to process an individual's personal data for generation and issuance of vaccination and recovery certificates.

The following lawful basis in Article 6 and Article 9 of the GDPR are appropriate and suitable for the purposes of processing personal data for the generation and dissemination of the Digital Covid Certificate (Vaccination & Recovery).

Article 6 (Lawfulness of processing)

- Processing is necessary to comply with a legal obligation to which the controller is subject (Article 6.1(c); (processing is necessary for compliance with a legal obligation to which the controller is subject).

Article 9 (Processing of special categories of personal data)

Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9.2(g); (Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject).

8.2 Lawful basis for processing of personal data by the Call Centre

Further to the above, the following lawful basis in Article 6 and Article 9 of the GDPR are also appropriate and suitable for the processing of personal data by call centre attendants on behalf of DoH/HSE in reference to amendment requests to pre-existing data sets and capture of additional personal data.

Article 6 (Lawfulness of processing)

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6.1(e); (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller).

Article 9 (Processing of special categories of personal data)

- Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (Article 9.2(g); (Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject).

8.3 Legislative Framework

The proposed data processing relates to all individuals in the Republic of Ireland that are administered the COVID-19 vaccination by the HSE and those who have been recorded has having recovered from Covid-19.

While the lawful basis for the processing of personal data for the Digital Covid Certificate is detailed in Article 6 and Article 9 of GDPR, it is helpful to set out legislative provisions that also support such processing by the Department of Health and the Health Service Executive:

- REGULATION (EU) 2021/953 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.

8.4 Exercise of Data Subject Rights

Under certain circumstances, data subjects have the following rights:

- **Right of access** – the right to request a copy of personal data held on a given data subject by the data controller.
- **Right to rectification** – the right to correct data that is inaccurate or incomplete.
- **Right to be forgotten** – the right, in certain circumstances, to have data erased. Typically, this does not apply to health care records and is not an absolute right.
- **Right to restriction of processing** – where certain conditions apply, such as in the event of known inaccuracies, the right to restrict the further processing of personal data until such time as the issue is resolved.
- **Right of portability** – where certain conditions apply, the right to have personal data transferred to another organisation.
- **Right to object** – the right to object to certain types of processing

To exercise any of these rights, please submit a request to the Health Service Executive. These details are available in Appendix E. Alternatively, requests may be submitted via the DCC Call Centre Support Service. When submitting a request, individuals may be required to provide additional information to confirm their identity.

Once the data subject's identity has been confirmed, the HSE will supply the data subject's information free of charge. However, a reasonable fee may be charged where the request is considered clearly unfounded, excessive or repetitive.

8.5 International Transfers

Insofar as the generation and issuance of the digital covid certificate is concerned, personal data will be processed primarily within the European Economic Area.

International transfers of personal data to third countries outside of the EEA not covered by an adequacy decision are foreseen in extremely limited circumstances such as:

- In the event of a system error, technical support provided by Microsoft with regard to Microsoft Azure may require access to the HSE environment which in turn may involve limited access to the personal data contained therein.
- In the event of a system error, technical support provided by Amazon with regard to AWS may require access to the DPER environment, which in turn may involve limited access to the personal data contained therein.

While the above instances of access are unlikely to occur in practice, the HSE have entered into appropriate data processor agreements incorporating standard contractual clauses with all relevant data processors to ensure such access remains in compliance with the GDPR and Data Protection Act 2018. In turn, these contracts stipulate that any data sub-processors engaged by the immediate contracting parties are entered into similar agreements offering a consistent level of protection.

8.6 Appointment of Data Processors

All data processors are appointed under appropriate and robust Data Processor Agreements in compliance with Article 28 of the GDPR.

8.7 Technical & Organisational Measures

The DoH/HSE, and DPER have each implemented a number of technical and organisational measures to protect the integrity, availability and confidentiality of personal data processed for the Digital Covid Certificate. The HSE environment, wherein all underlying personal and special category data is stored and originates for this project, is hosted on the secure Microsoft Cloud (i.e. Microsoft Azure & CRM Dynamics) and within Microsoft data centres located within the European Economic Area (EEA).

In turn, the DPER environment, wherein all personal and special category data will be transferred in order to generate the Digital Covid Certificate, is hosted on a secure Amazon Web Services cloud and within AWS data centres located within the European Economic Area.

The DoH, HSE and their associated data processors shall ensure that their employees, agents, representatives, and contractors involved in the project are appropriately trained with regard to their individual and corporate data protection responsibilities.

The underlying systems leveraged in generating the Digital Covid Certificate provide substantive assurances as to the end-to-end security of personal and special category data processed therein. A number of technical features and process controls have been implemented to ensure the integrity of the data. Examples of such measures are as follows:

- Role-based security model for all operating environments with restricted access
- Segmentation of generation and sync jobs to combat potential network latency issues
- Secure APIs for transfer of data between environments
- Secure QR code generation and validation security review
- Encryption of data in transit between environments
- Encryption of data at rest within a given environment
- Full penetration testing across all potential access points

9. Identify, Assess and Mitigate Risks

The table below sets out the risks that have been identified for the project and the levels for those risks if not mitigated. Overall risk score for each risk identified is calculated as the product of the risk likelihood score and the risk impact score (i.e. likelihood score X impact score).

An evaluation of the identified risks has also been carried out and a series of measures have been detailed that seek to mitigate those risks to an acceptable level. It is most important to understand that the purpose of risk management is to identify all possible risks so that that their potential impact and level of likelihood can be assessed and then mitigated by taking appropriate actions. For that reason, it is the post mitigated risk measure that is relevant.

Likelihood	Score	Impact	Score	Overall	Score
Highly Unlikely	**1**	Negligible	**1**	Low	**1 - 7**
Unlikely	**2**	Minor	**2**		
Possible	**3**	Moderate	**3**	Medium	**8 - 14**
Likely	**4**	Major	**4**		
Highly Likely	**5**	Critical	**5**	High	**15 - 25**

No.	Risk	Likelihood	Impact	Likelihood Score	Impact Score	Overall Risk	Measures to Mitigate Risk	Likelihoodwith measureres	Impactwith measures	ResidualRisk	Remaining risk to data subjects
1	Risk of insecure methods of data transfer used that allow access to patient data transferred to Department of Public Expenditure and Reform (OGCIO)	Due to the pace of the wider project, it is possible that this risk may come to fruition.	Critical. While the content of the JSON/Manifest files contain limited special category data, there is ability to leverage this data to the detriment of the data subject. Particularly given the scale of the processing involved, this further increases the impact of a successful attempt.	3	5	15	Ensure data is encrypted in transit over the network and encrypted at rest. Test to ensure that encryption is effective.	1	5	5	Virtually impossible to intercept data if these controls are implemented.
2	Risk of the IIS data lake being hacked to obtain patient information.	It is likely that attempts will be made to hack into the respective system.	Access to data held within the wider data lake, CoVax or CCT may result in instances of identity theft, phishing and smishing attacks. Following the recent cyber-attack, another breach of this nature would further undermine public trust.	3	5	15	HSE has implemented a number of technical and operational measures. Regular tests to ensure that measures implemented are effective.	1	5	5	Once implemented and tested on a regular basis, the likelihood of this risk coming to fruition is greatly reduced.
3	Risk that users are not given sufficient information in the Digital Covid Certificate programme, what data will be further processed from Covax/CCT and for what purpose in a comprehensive way.	The requirement to have excellent communications about the DCC is understood though the pace of the wider project increases likelihood that DPIN notices will go unchecked.	If appropriate information is not provided in a comprehensive and timely manner, this may constitute a breach of the transparency principle. As the initial batches of the DCC will be pushed out rather than requested, this may result in a series of complaints from disenfranchised cohorts.	3	3	9	Devise a communication strategy to ensure all relevant information is readily accessible by the wider public.	1	3	3	Where sufficient information is provided, this risk will be fully mitigated.

4	Retention of JSON/Manifest Files – DoH/HSE If a retention period isnot established information might be retained for longer than necessary.	It is unlikely that information will be held longer than the agreed retention period.	Breach of the storage limitation principle by DoH/HSE. Breach of the purpose limitation principle by DoH/HSE. Administrative fines from the Regulator Reputational damage.	2	3	6	Establish an appropriate and proportionate retention schedule for JSON/Manifest files post transfer to DPER (OGCIO)	2	3	6	Provided that appropriate data quality measures are incorporated, this will result in negligible risk to data subjects.
5	Duplicate data held in IS data lake: Where JSON/Manifest files are retained within the IS data lake past the point of generation and transmission to DPER, this would result in duplicate and potentially misaligned data sets.	It is unlikely that JSON/Manifest files will be retained by the HSE/DoH for an extensive period of time.	In the absence of a clear and proportionate purpose for retention, this would surmount to a breach of the data minimization and storage limitation principles of the GDPR.	2	3	6	Establish an appropriate and proportionate retention schedule for JSON/Manifest files post transfer to DPER (OGCIO)	1	3	3	Provided that retention schedules are created and abided by, this risk will be resolved
6	Excessive personal data processed by the HSE to generate JSON/Manifest files: While the DCC Regulation provides the minimum data fields required to generate a given certificate, review by the EDPB/EDPS highlights a lack of substantive assessment as to the necessity of each data field.	It is unlikely that JSON/Manifest files will contain what might be deemed 'excessive' amounts of personal data.	Excessive information would contravene the proposed DCC Regulation which is relied upon as the lawful basis for generation and distribution of the DCC. This would ultimately equate to a breach of the data minimization and purpose limitation principle in light of currently known purposes for generation of the DCC.	2	3	6	Review each data field for proportionality and ensure clear and substantive reasoning for processing is considered and understood.	1	3	3	Where each data field has been assessed for proportionality and aligns with the underlying purpose for processing, this risk will be mitigated
7	Inaccurate vaccination data: A significant number of GPs, when administering a vaccine and logging details of same within Covax, clicked the first option available within the drop-down list of vaccines (AstraZenica), regardless of what vaccine was genuinely administered. This results in inaccurate vaccination data flowing from Covax into the IS data lake and may result in the generation of false DCCs downstream.	This is a known issue effecting multiple records and so the risk likelihood is high.	This would surmount to a breach of the accuracy principle. Where inaccurate data is processed to generate the DCC further downstream, this could potentially result in members of the public being unable to benefit from the DCC, which in turn may lead to complaints and reputational damage for the DoH/HSE.	5	4	20	Implement internal measures to assess and amend vaccination records through Covax. Engage with the wider GP community to ensure records are updated in line with available batch numbers. Implement a flagging system which only allows approved records from Covax to generate a vaccination certificate. Flag updated files to ensure DPER can distinguish between certificates issued.	2	4	8	Implementing appropriate review measures will reduce the total number of inaccurate records in Covax. However, given the total number of records involved, and the potential consequence of errors, some residual risk remains.
8	Inaccurate recovery data: Broad assumptions are being made that recovery data flowing from CCT into the IS data lake is accurate. There is no formal review process to flag records as being fit for purpose. This may result in the generation of inaccurate DCC's further downstream.	In the absence of a formal review process, the likelihood of inaccurate data being processed to generate a recovery certificate is high.	This would surmount to a breach of the accuracy principle. Where inaccurate data is processed to generate the DCC further downstream, this could potentially result in members of the public being unable to benefit from the recovery DCC, which in turn may lead to complaints and reputational damage for the DoH/HSE.	4	4	16	Implement data quality review procedures for recovery stream data. Add a DCC ready flag as with the vaccination stream.	2	4	8	Implementing appropriate review and flagging measures will reduce the total number of inaccurate records in CCT and thus the wider data lake. However, given the total number of records involved, some residual risk remains.
9	Vaccination Stream - Data Quality Flagging System: Where Covax records are initially tagged/flagged as being DCC ready by the Data Quality team and then subsequently untagged, there is no process to indicate this change to the IIS team. This may hamper IIS' ability to update the HSE Live call centre with relevant information.	While it is expected that this scenario will only be applicable in limited circumstances, in the absence of a mechanism to highlight removal of the 'DCC Ready' tag from a previously issued file, the likelihood of this risk coming to fruition is considered high.	Where the DCC call centre is not provided with up-to-date information, this may prevent data subjects from receiving information regarding the status of their DCC from the call centre in a timely manner.	4	3	12	Implement notification capability allowing IIS to fully update DCC call centre records with any material changes made regarding a files' eligibility.	1	3	3	Implementing a notification system would effectively mitigate this risk and allow the DCC call centre remain abreast of all material changes to a given individual's Vaccination DCC eligibility.
10	Data Subject Rights – Rectification: HSE Live will flag data quality issues to the HSE for resolution. However, there is a risk that a formal rectification request may be raised and no operating procedure exists to appropriately capture and respond to the request. SOPs are required to formally record these requests in line with the respective parties' accountability obligations and to ensure that all requests of this nature are actioned within the statutory timeframes.	It is possible that a formal rectification request will be received via the call centre.	Lack of a formalised methodology may result in rectification requests being missed or otherwise unfulfilled within the statutory timeframe of one calendar month. This would represent a breach of data subject rights which in turn may result in a complaint being made to the Regulator.	3	3	9	Ensure that call centre attendees have been briefed on the DoH/HSE's rectification request procedure and implement pathways to flag and process formal rectification requests as they arise.	1	3	3	Where appropriate SOPs are implemented, risk likelihood will be mitigated.

11	Data Subject Rights – Access: SOPs are required outlining the appropriate response in the event that the HSE Live call centre receives a formal subject access request. In the absence of same, there is a risk that a formal subject access request will be raised and no operating procedure exists to appropriately capture and respond to the request	It is likely that the HSE Live call centre will receive the occasional formal subject access request from data subjects.	Lack of a formalised methodology may result in access requests being missed or otherwise unfulfilled within the statutory timeframe of one calendar month. This would represent a breach of data subject rights which in turn may result in a complaint being made to the Regulator.	4	3	12	Ensure that call centre attendees have been briefed on the DoH/HSE's access request procedure and implement pathways to flag and process formal access requests as they arise.	1	3	3	Where appropriate SOPs are implemented, risk likelihood will be mitigated.
12	HSE Live Call Centre - Recording of Notes: In responding to members of the public, call centre attendants may generate physical/digital notes on a given query that contains additional personal data. Where call centre attendees are working remotely from home, generation of notes in physical form represents a potential security risk.	It is likely, in the absence of clear guidelines that this practice will occur.	Where notes are lost or improperly disposed of, this may result in a reportable data breach due to the special category data potentially captured.	4	3	12	Ensure that clear guidance is provided to HSE Live with regard to taking of physical/digital notes. This guidance should instruct call centre agents to ensure that any notes taken during support calls are relevant, proportionate and appropriately secured.	2	3	6	Clear guidelines will reduce the likelihood of unnecessary note taking and the associated security risks associated with same.
13	DPIN Notice Update – Covax: The current DPIN for Covax does not include material details outlining further processing for the purpose of generating the DCC.	At time of writing, this is currently the case.	Where inadequate information is provided, this will constitute a breach of the transparency principle. Individuals may be surprised and concerned that their personal data originally captured for one purpose is now being used for a new, though not incompatible, purpose.	5	3	15	Update DPIN notice to reflect further processing of personal and special category data for the purpose of generating the Digital Covid Certificate	1	1	1	Once updated, this risk is effectively mitigated. DPIN notices should remain under review throughout the course of the project to ensure any changes to processing are captured.
14	Updates to Record of Processing Activity (RoPA) – HSE: In line with Art. 30 of the GDPR, the HSE will need to update their RoPA to account for new processing activities encompassed within this project. Given the pace of the wider project, there is a risk that this requirement will go unchecked.	Given the pace of the wider project, it is possible this requirement may be overlooked.	Where RoPA's fail to robustly account for the processing activities undertaken by the data controller, same will be in breach of Art. 30 and may result in sanctions being imposed by the Regulator.	3	2	6	Update Records of Processing Activity to reflect processing of personal and special category data for the purpose of generating the Digital Covid Certificate in its various streams.	1	1	1	Once updated this risk is essentially mitigated though the RoPA should remain under review to account for any further evolutions in the Digital Covid Certificate scheme.
15	Updates to Record of Processing Activity (RoPA) – DoH: In line with Art. 30 of the GDPR and as mandated under the Accountability principle, the DoH will need to update their RoPA to account for new processing activities encompassed within this project. Given the pace of the wider project, there is a risk that this requirement will go unchecked.	Given the pace of the wider project, it is possible this requirement may be overlooked.	Where RoPA's fail to robustly account for the processing activities undertaken by the data controller, same will be in breach of Art. 30 and may result in sanctions being imposed by the Regulator.	3	2	6	Update Records of Processing Activity to reflect processing of personal and special category data for the purpose of generating the Digital Covid Certificate in its various streams.	1	1	1	Once updated this risk is essentially mitigated though the RoPA should remain under review to account for any further evolutions in the Digital Covid Certificate scheme.
16	Joint Controller Agreement – DoH/HSE: In line with Art.26 of the GDPR, the Department of Health and Health Service Executive, as the entities jointly determining the purpose and means of processing personal data with regard to the generation and delivery of the DCC, must enter into an 'arrangement' outlining their respective roles and responsibilities	Given the pace of the wider project, it is possible this requirement may be overlooked.	Failure to substantiate the relationship via an appropriate agreement may result in ineffective delivery of information to the respective data subjects as mandated under Art.13 and Art.14 of the GDPR. In turn, this may result in data subject right invocations going unanswered.	3	4	12	Implement an appropriate agreement outlining each party's respective roles and responsibilities, paying particular regard to information delivery and upholding data subject rights.	1	1	1	Once implemented, this risk is effectively resolved. However, should the position change with regard to the testing stream of the DCC, this agreement should be appropriately revised to capture same.
17	Data Processing Agreement – Department of Public Expenditure and Reform: As joint data controllers for the wider purpose of delivering the DCC, the Department of Health and Health Service Executive are mandated under Art.28 of the GDPR to enter into a data processor agreement with the Department of Public Expenditure and Reform prior to transfer of any personal data.	Given the pace of the wider project, it is possible this requirement may be overlooked	Failure to enter into an appropriate data processor agreement with the Department of Public Expenditure and Reform (DPER) would surmount to a breach of Art.28 GDPR which in turn may result in penalties issued by the Regulator and wider reputational damage	3	4	12	Implement an appropriate data processor agreement with the Department of Public Expenditure and Reform in line with Art.28 of the GDPR.	1	1	1	Once implemented, this risk is effectively resolved.
18	Due-Diligence - Department of Public Expenditure and Reform (DPER): As Joint Data Controllers, the Department of Health and Health Service Executive are obligated under Art.28 to perform appropriate due diligence checks with regard to their intended data processor, the Department of Public Expenditure and Reform.	Given the pace of the wider project, it is possible this requirement may be overlooked.	Where data controllers fail to undertake the requisite due diligence checks on their data processors, this may result in administrative fines in the event of an investigation by the Regulator. Further to the above, failure to perform the requisite security checks in advance of engaging DPER may ultimately result in a data breach which could undermine public confidence in the wider DCC programme.	3	4	12	Undertake appropriate and proportionate due-diligence exercise with DPER.	1	1	1	Once complete and responses are deemed acceptable by the joint controllers, this risk is effectively resolved. However, if an inadequate response is tendered, the joint controllers are obligated under Art.28 to disengage.

19	Data Processing Agreement – Ernst and Young (EY): As joint data controllers for the wider purpose of delivering the DCC, the Department of Health and Health Service Executive are mandated under Art.28 of the GDPR to enter into a data processor agreement with Ernst and Young (EY) prior to transfer of any personal data.	Given the pace of the wider project, it is possible this requirement may be overlooked.	Failure to enter into an appropriate data processor agreement with the Ernst and Young would surmount to a breach of Art.28 GDPR which in turn may result in penalties issued by the Regulator and wider reputational damage	3	4	12	Implement an appropriate data processor agreement with EY in line with Art.28 of the GDPR.	1	1	1	Once implemented, this risk is effectively resolved.
20	Due-Diligence – Ernst and Young (EY): As Joint Data Controllers, the Department of Health and Health Service Executive are obligated under Art.28 to perform appropriate due diligence checks with regard to their intended data processor, Ernst and Young (EY).	Given the pace of the wider project, it is possible this requirement may be overlooked.	Where data controllers fail to undertake the requisite due diligence checks on their data processors, this may result in administrative fines in the event of an investigation by the Regulator. Further to the above, failure to perform the requisite security checks in advance of engaging EY may ultimately result in a data breach which could undermine public confidence in the wider DCC programme.	3	4	12	Undertake appropriate and proportionate due-diligence exercise with EY.	1	1	1	Once complete and responses are deemed acceptable by the joint controllers, this risk is effectively resolved. However, if an inadequate response is tendered, the joint controllers are obligated under Art.28 to disengage.
21	Risk that data will be transferred/accessed outside the EEA.	Services such as Amazon Web Services and Microsoft Azure include technical support that may require access from a third country in certain, limited circumstances.	Data controllers and data subjects may not be able to fulfil/avail of their data protection obligations and rights.	2	4	8	Incorporate standard contractual clauses with relevant data processors that provide sufficient guarantees as to the integrity of personal data and ability to fully exercise data subject rights.	2	2	4	Data may still be processed sporadically outside the EEA though subject to safeguards incorporated via standard contractual clauses.
22	Risk of ineffective data breach procedures – Data Processors:	Given the pace of the wider project, it is likely this requirement will be overlooked.	Where effective, cohesive data breach procedures are absent, this may result in a number of potentially damaging outcomes such as failure to escalate a given breach to the data controller, delayed reporting to the regulator, ineffective breach mitigation measures or failure to notify the respective data subjects (where applicable).	4	5	20	Ensure all data processor contracts capture data breach protocols and outline the obligation to escalate an identified breach to the data controllers without undue delay. Ensure appropriate and cohesive data breach SOPs are implemented by all parties and are fully understood. Ensure all breaches are appropriately logged for audit purposes.	2	5	10	Once implemented and understood the likelihood of this risk coming to fruition is reduced. However, there remains a residual risk that relevant parties will fail to follow protocol.

10. Sign off and Record Outcomes

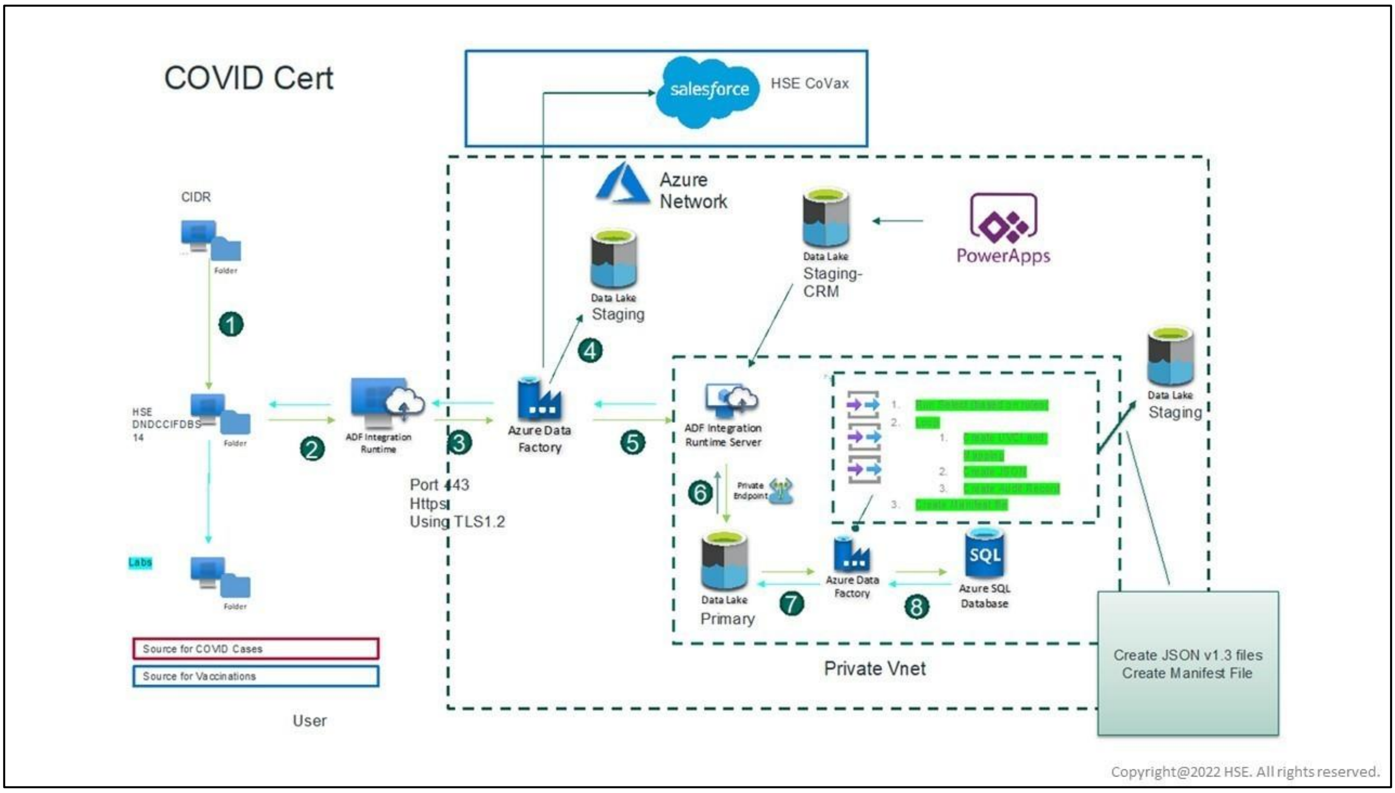
Item	Name/Date	Notes
Risk measures approved by:	Damien McCallion (HSE) – 27/07/2021 Muiris O'Connor (DoH) – 23/07/2021	
Residual risks approved by:	Damien McCallion (HSE) – 27/07/2021 Muiris O'Connor (DoH) – 23/07/2021	
HSE DPO advice provided:	Jim O'Sullivan – 27/07/2021	Having been actively involved from the outset in the group which developed the DPIA for the Digital Covid Certificate (DCC) [Vaccination and Recovery formats] on behalf of the Joint Data Controllers, I have now considered the final draft document as approved by the senior responsible officers in HSE and Department of Health (DoH). The issuing of these certificates is in accordance with EU DCC Regulations (Regulation (EU) 2021/953) to help citizens move freely and safely within the EU during the COVID-19 pandemic and I am satisfied that the appropriate lawful basis for processing of data for this purpose has been established. I note that the use of the DCC for other purposes is dependent on separate legislation and does not fall within the scope of this DPIA. In accordance with Article 35(7) GDPR, the DPIA sets out a systematic description of the purpose of the relevant processes; the necessity and proportionality of these; an assessment of the risks involved, and the measures envisaged to address such risks. In my opinion due consideration has been given to the relevant data privacy, security and protection issues and the necessary agreements have been put in place by the HSE and DoH in accordance with Articles 26 and 28 GDPR. I am aware of issues relating to the quality of some of the underlying data held in the HSE's IIS Data Lake and it is important that the on-going work to improve data quality continues and that any data breaches and incidents resulting from the DCC process are managed appropriately. I note a good degree of information and transparency in relation to the process of generating and obtaining a digital certificate. All relevant material should be kept under review to ensure that it reflects any changes as the

		programme progresses to ensure good public information. I recommend that all relevant staff and contractors interacting with personal data should be aware of the fundamentals of GDPR and undertake appropriate training so that all of those involved are aware of relevant considerations and act appropriately in relation to this personal data. Accordingly, my opinion from a data privacy and protection perspective it is that it is in order to continue with the process of issuing Digital Covid Certificates in the Vaccination and Recovery Formats. While the DPIA acknowledges the existence of a third-party operated call centre facility, the workings of this call centre were not considered during the preparation of this DPIA as they were evolving at the time. I am also becoming aware of the opening of an on-line “self-service” portal. I strongly recommend that a separate DPIA be conducted focusing specifically on the operations of the call centre and the portal from a data protection and privacy perspective. Updated 12/12/2022: The National DPO Office received the Issuance of Digital COVID Certificate (Vaccination Recovery) DPIA on 07/12 which has been updated as HSELive have taken on the customer service provision for the Digital COVID Certificates. We are satisfied with the amendments made to this DPIA. We request that you contact the National DPO Office should there be any further changes to the processing activity.
DoH DPO Advice Provided:	Mary Saunderson – 28/07/2021	EU Regulation 2021/953 provides for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test, and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic. The certificates will only include the minimum amount of personal data that is necessary for this purpose. The Department of Health and the Heath Service Executive (HSE) are the authorities tasked with generating and issuing the Digital Covid Certificate (DCC) in Ireland and are Joint Controllers for this process under the GDPR. The Department of Health and HSE will issue either a digital or physical DCC to all relevant members of the public. This DPIA covers the generation and delivery of the DCC for vaccination and recovery streams only. The EU Regulation also recognises that Member States may choose to use the Digital Covid Certificate for purposes other than travel, this would require a distinct legislative framework and is also outside

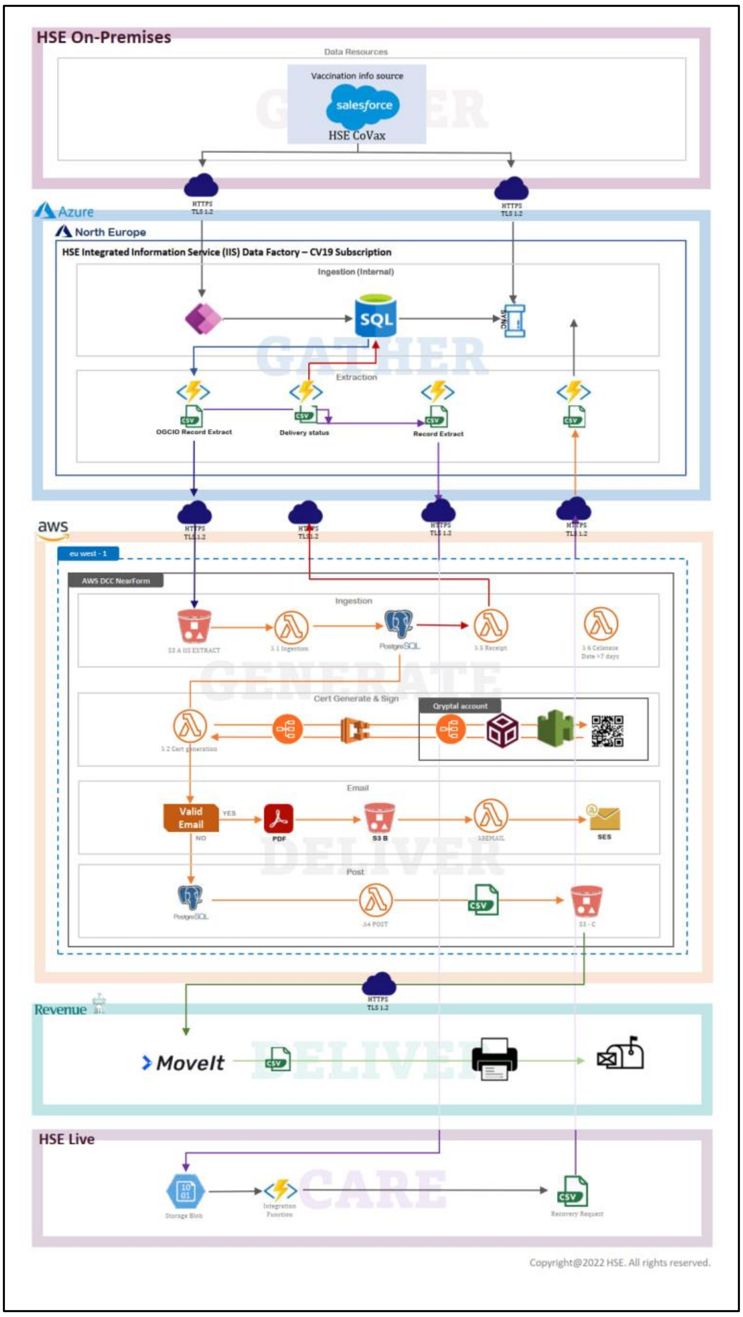
		the scope of this DPIA. As the DCC programme is large scale processing and the personal data contained in the certificates includes special category health data, a high level of data protection is required. All the principles of data protection must be adhered to. I note that a lot of work has been carried out in this regard by the team involved and that there has been consultation with the DPC. The DPIA identifies the legal basis for the processing of personal data for the generation and dissemination of the DCC (Vaccination & Recovery) and by the Call Centre. This is underpinned in national and EU law. I note that a Joint Data Controller Arrangement between the Department and the HSE under Article 26 of the GDPR has been signed. Article 28 Data Processing Agreements must be completed with all relevant data processors. I note that several risks have been identified and that safeguards are outlined to address and reduce the risk to individuals' personal data. These controls will need ongoing monitoring and review. The principles of necessity, proportionality and data minimisation have been considered and adhered to. From a transparency and public trust viewpoint, there should be clear communication with data subjects on the purpose of the processing and security in place to protect their personal information. It is important that data subjects have a clear point of contact to exercise their data protection rights easily and avoid personal data being duplicated unnecessarily. SOPs also need to be developed and implemented for the Call Centre to ensure all data subjects rights are protected. I note that there are various retention limits on different types of personal data being processed for the generation and issuance of the DCC, an appropriate retention schedule needs to be put in place as soon as possible. I also note that a risk in relation to inaccurate vaccination data has been identified and that appropriate review measures will be implemented to address this. In relation to the processing of children's personal data, at present the DCC will not be

		issued to under 18s, should this policy change the DPIA will need to be updated. As this DCC programme has been implemented at a very quick pace and will continue to evolve, the DPIA should be reviewed and updated to reflect any material changes to the processing as this project progresses. 14/12/2022 – I have reviewed the DPIA for the DCC programme, which has been updated to reflect that the call centre support service will now be operated by HSELive. I am satisfied that this change is in order from a data protection perspective. The processing of personal data for the DCC (Vaccination & Recovery) should be kept under review as the public health situation changes.
DPO advice accepted or overruled by:	Accepted by Damien McCallion (HSE) and Muiris O'Connor (DoH)	
This DPIA will be kept under review by:	Damien McCallion (HSE) and Peter Lennon (DoH)	

11. Appendix A – Collation of personal data from HSE sources



12. Appendix B –Generation of DCCs (Vaccination and Recovery)



13. Appendix C – Digital Covid Certificate Governance Group

1. Role and Purpose:

The HSE DCC Governance Group consists of work-stream leads from the HSE and contracted delivery partners where appropriate.

The group have the following roles and responsibilities: -

- Act as the decision-making and approval body relating to the data delivery to support the DCC Program
- Review, advise and approve key decisions in a timely manner.
- Provide governance and oversight with regards to data rules, quality, transfer and data protection and governance.
- Ensure appropriate linkage with other stakeholder and reference groups.
- Resolve all issues in a timely manner
- Escalation to the Department of Health where appropriate

The work of the Group is informed by legislation, regulation, government policy, strategies and operational plans for various services within-scope.

2. Membership:

The HSE Digital Covid Certificate Governance Group membership is as follows:

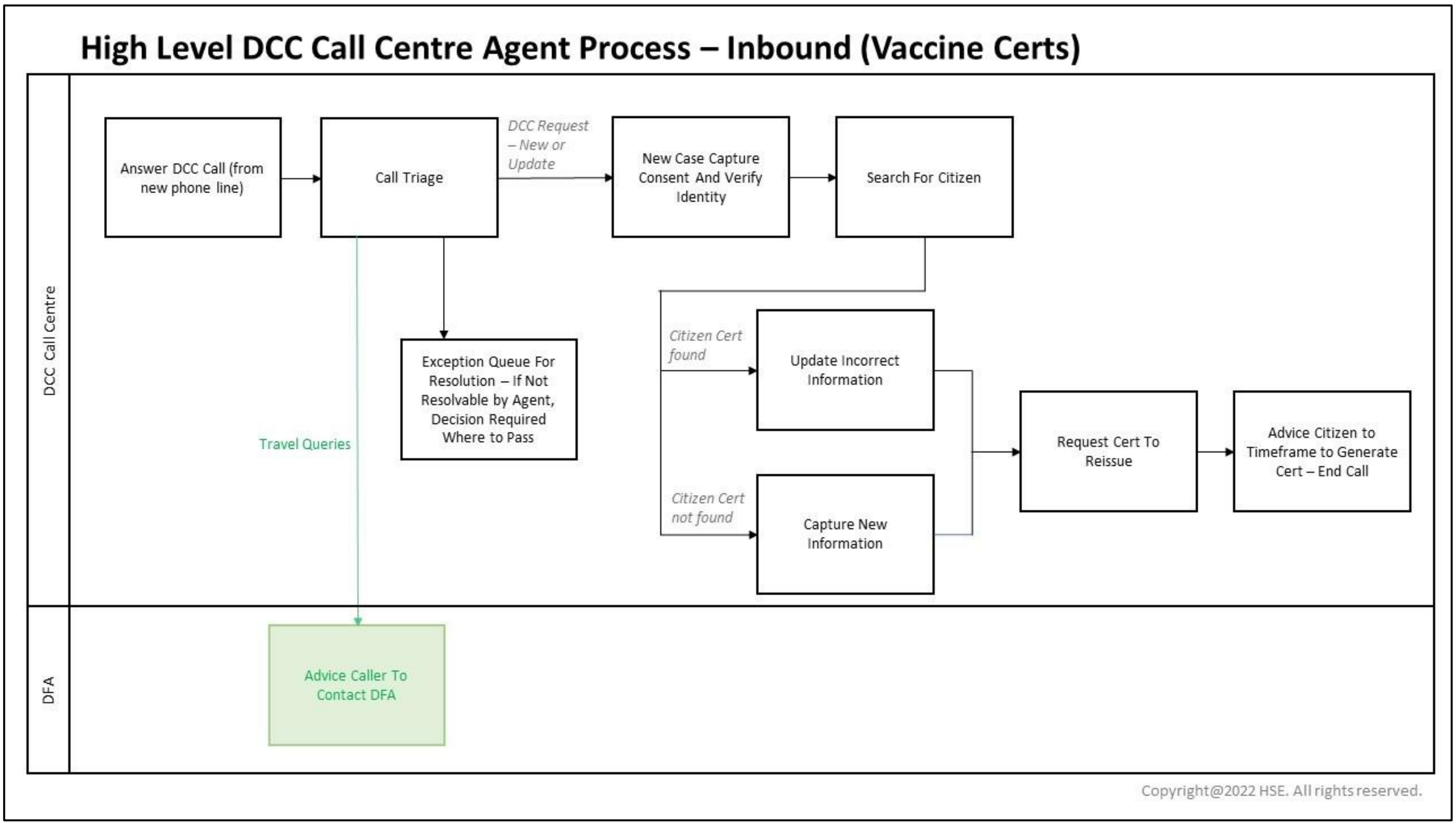
Membership:
Niall Sinnott, Department of Health
Ben Cloney, HSE Digital
Carmel Cullen, HSE Live
Eileen Whelan, HSE Test, Trace & Vaccination
Fran Thompson, HSE Chief Information Officer
Mark Bagnall, IIS
Johnny Farren, Acting DPO and Head of Data Protection
Gary Comiskey, PMO

The group may, if circumstances require, co-opt other relevant experts throughout the duration of the project.

3. Meetings:

The HSE DCC Governance Group will meet as required throughout the implementation phases of the Programme.

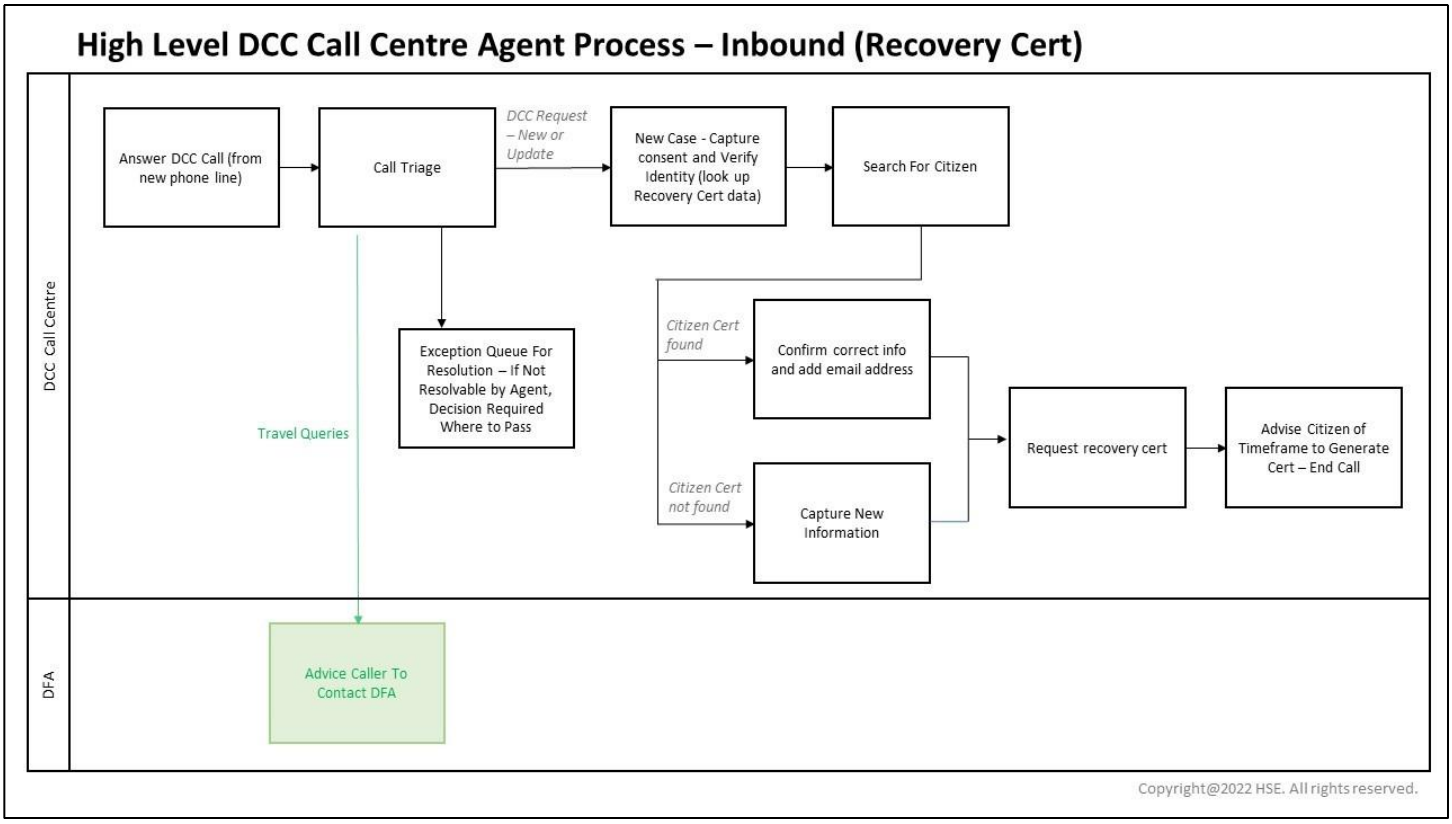
14. Appendix D –Data Flow Chart for Call Centre Support Service



High Level DCC Call Centre Agent Process – Inbound (Vaccine Certs)

DCC Call Centre
DFA
Answer DCC Call (from new phone line)
Call Triage
DCC Request – New or Update
New Case Capture Consent And Verify Identity
Search For Citizen
Exception Queue For Resolution – If Not Resolvable by Agent, Decision Required Where to Pass
Travel Queries
Citizen Cert found
Update Incorrect Information
Citizen Cert not found
Capture New Information
Request Cert To Reissue
Advice Citizen to Timeframe to Generate Cert – End Call
Advice Caller To Contact DFA

Copyright@2022 HSE. All rights reserved.



High Level DCC Call Centre Agent Process – Inbound (Recovery Cert)

DCC Call Centre
DFA
Answer DCC Call (from new phone line)
Call Triage
DCC Request – New or Update
New Case - Capture consent and Verify Identity (look up Recovery Cert data)
Search For Citizen
Exception Queue For Resolution – If Not Resolvable by Agent, Decision Required Where to Pass
Travel Queries
Citizen Cert found
Confirm correct info and add email address
Citizen Cert not found
Capture New Information
Request recovery cert
Advise Citizen of Timeframe to Generate Cert – End Call
Advice Caller To Contact DFA

Copyright@2022 HSE. All rights reserved.

15. Appendix E –Data Protection Officer and Deputy Data Protection Officer Contact Details

Contact Details for HSE Data Protection Staff are as follows:

Data Protection Officer (DPO) HSE	Email: dpo@hse.ie Telephone: 087 - 908 2160
Deputy Data Protection Officer West (excluding voluntary agencies) • CHO 1 – Cavan, Donegal, Leitrim, Monaghan, Sligo • CHO 2 – Galway, Mayo, Roscommon • Mid-West Community Healthcare • Saolta Hospital Group	Email: ddpo.west@hse.ie Telephone: 091-775 373
Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitalsand agencies) • Midlands, Louth, Meath Community Health Organisation • Community Health Organisation Dublin North City & County • CHO 6 – Dublin South East, Dublin South & Wicklow • RCSI Hospital Group	Email: ddpo.dne@hse.ie Kells Office: :046-9251265 Cavan Office: 049-4377343
Deputy Data Protection Officer Dublin mid-Leinster (excluding voluntary hospitals and agencies) • Dublin Midlands Hospital Group • Ireland East Hospital Group • Community Healthcare Dublin South, Kildare & West Wicklow	Email: ddpo.dml@hse.ie Tullamore Office: 057-93 57876 Naas Office 045-880496
Deputy Data Protection Officer South (excluding voluntary hospitals and agencies) • Cork & Kerry Community Healthcare • CHO 5 – Carlow, Kilkenny, South Tipperary, Waterford & Wexford • UL Hospital Group • South South-West Hospital Group	Email: ddpo.south@hse.ie Cork Office 021-4928538 Kilkenny Office 056-7785598

Contact Details for the Department of Health Data Protection Officer are as follows:

Data Protection Officer (DPO) DoH	Email: dpo@health.gov.ie Telephone: 01 635 4476