# NORTHERN IRELAND’S COVID CERTIFICATION SERVICE

# DATA PROTECTION IMPACT ASSESSMENT

|  |  |
| --- | --- |
| **DPIA Ref no. *(Information Governance to provide*)** | |
| **Version 1.2, 23rd Dec 2021** | |
| **Project Name** | |
| **COVID Certification Service** | |
| **Business Area** | |
| **DoH/HSCB/PHA** | |
| **Information Asset Owner** | **Project Manager** |
| **Dr Margaret O'Brien;**  **MB, BCh, BAO, MSc, FFCI**  **Assistant Director of Integrated Care**  **Head of General Medical Services**  **Responsible Officer HSCB**  **Dan West (DoH);**  **Dr Steven Bergin (PHA) Interim Director of Public Health and Personal Data Guardian** | **Dr Edward O’Neill**  **CCS Solution Manager**  **COVID Certification Service (CCS)** |

Contents

[1. DPIA COVID Certification Service 3](#_Toc91165147)

[Management 3](#_Toc91165148)

[The COVID Certification Service 3](#_Toc91165150)

[2. Purpose of the CCS 3](#_Toc91165151)

[3. COVID Certification Service 4](#_Toc91165152)

[CCS Overview 4](#_Toc91165153)

[CCS Development and Drivers 5](#_Toc91165154)

[4. CCS Roles and Responsibilities 8](#_Toc91165155)

[5. Consultation & Stakeholders 8](#_Toc91165156)

[CCS Governance 8](#_Toc91165157)

[6. Data Processing Overview and Scope 9](#_Toc91165158)

[Data Subjects 9](#_Toc91165159)

[Purpose of processing 9](#_Toc91165160)

[7. Context of Processing and Data Items Processed 10](#_Toc91165161)

[Use of Data 12](#_Toc91165162)

[8. Compliance with data protection law and other regulatory guidance 17](#_Toc91165163)

[The UK GDPR Lawful Basis for Processing 17](#_Toc91165164)

[Common Law Duty of Confidentiality 18](#_Toc91165165)

[Necessity and Proportionality 18](#_Toc91165166)

[CCS Data Retention 20](#_Toc91165167)

[Data Rights 20](#_Toc91165168)

[Prevention of CCS Scope/ Function Creep 21](#_Toc91165169)

[9. Security Measures 21](#_Toc91165170)

[CCS Information Security 22](#_Toc91165171)

[Security Controls in place for the CCS 22](#_Toc91165172)

[How we control users who has access to the CCS 22](#_Toc91165173)

[10. Identify and Assess Risks (what are the risks) 23](#_Toc91165174)

[11. Identify Measures to Reduce Risks 25](#_Toc91165175)

[Appendix A- CCS Stakeholder Landscape 32](#_Toc91165176)

[Appendix B - Data Processors 33](#_Toc91165177)

[Appendix C – Security Measures 35](#_Toc91165178)

# DPIA COVID Certification Service

|  |
| --- |
| ManagementA Covid Certification Service has been commissioned and will be managed by the Department of Health (DoH), Health and Social Care Board (HSCB) and Public Health Agency (PHA). These three organisations are therefore the joint data controllers of the CCS and will be assisted by a range of data processors - please refer to Appendix B - Data Processors in this document for further information. NI Direct and key suppliers have been employed to help deliver CCS.The COVID Certification Service |

This DPIA relates to the NI COVID Certification Service (CCS) and describes the process within Northern Ireland to generate COVID Certificates for all eligible citizens that can be used for the purpose of international travel and domestic use cases. There is a separate DPIA to cover the processing involved with the CovidCert Check NI Verifier App, which can be read in conjunction with this DPIA.

# Purpose of the CCS

As the success of the vaccination programme continues, pressure is increasing to ease restrictions. As international travel resumes, it is assumed that there will be a requirement for travellers to share immunity status and/or testing status as a condition for entry into countries they are travelling to. As lockdown restrictions are removed, there is increased domestic movement outdoors and in closed venues (see full list below in Section 3 for domestic use cases), and in order to assure safety of all and reduce the opportunity for transmission from person to person, there can be requirements for visitors to share their vaccination status for entry into these venues.

As the standards for secure documentation are confirmed by the EU and World Health Organisation (WHO) it has become clear that GPs and HSC Trusts are unable to provide documentation to the required, secure standard. Therefore, solutions that can provide the required assurances to agreed international standards are needed, hence the development of COVID Certification Service (CCS) and associated mobile (COVIDCERT NI) App.

The Department of Health (DoH), Regional Health and Social Care Board (HSCB) and Public Health Agency (PHA), are Joint Data Controllers for the personal information processed in the CCS and mobile App.

# COVID Certification Service

## CCS Overview

aThe Department of Health, Health and Social Care Board and Public Health Agency, through the Digital Health and Care NI (DHCNI) team, have worked jointly on the development and delivery of a COVID Certification Service and associated App that, by virtue of vaccination, facilitates international travel (meeting EU and WHO requirements) and domestic use cases. The Department of Finance through NI Direct, as well as other key suppliers, have been employed to help deliver the CCS and COVIDCERT NI App.

The requirement to use the Covid Certification Service to provide evidence of your Covid status is currently required by most private sector organisations such as airlines, cruise ships and holiday operators to allow access to their services for international travel; similarly, for domestic use cases requirements have been put in place for:

* Indoor events (where some or all of the audience are not normally seated) with 500 or more attendees
* Outdoor events (where some or all of the audience are not normally seated) with 4,000 or more attendees
* events where more than 10,000 people will be present, regardless of whether or not they will be seated
* Nightclubs
* Licensed Hospitality premises and unlicensed premises for the duration of the time when they are operating under an occasional licence or when BYO alcohol is consumed
* Cinemas, theatres and conference halls

The EU eHealth Network has published an outline of the trust framework required for a Digital Green Certificate infrastructure and has prepared technical specifications for the mutual recognition and interoperability of vaccination, test and recovery certificates. Finally, the CCS solution protects Health Service, such as GPs, from being burdened with requests for details of immunisation and test data.

The CCS solution provides citizens with an easily accessible, streamlined process for obtaining a certificate. Additionally, this removes the requirement for GPs and healthcare organisations to manage requests for proof of immunisation and test data, thereby freeing them to concentrate on direct patient care.

* The scope of the CCS covers both a digital and paper-based solution for people to obtain trusted, and internationally accepted COVID status certification, based on their vaccination information, testing information or recovery from Covid following positive PCR, for use in international travel settings and domestic use cases.

CCS can also be used by citizens who qualify for a medical exemption from vaccination and wish to obtain a certificate. Exemption guidance can be found on the [NIDirect website](http://www.nidirect.gov.uk/covid-exemption-certificate).

## CCS Development and Drivers

The primary objective of the COVID Certification Service is to enable individuals to access and share their COVID immunisation and / or testing data in the manner required for international travel from Northern Ireland and for Domestic use cases within Northern Ireland, in line with the developing EU Trust Framework (Digital COVID Certificate) and WHO published standards.

The ability to prove a citizen is COVID safe is achieved by obtaining the current COVID eligibility status based on their COVID records. The objective for the service design and the solution architecture are to:

* Use global standards to enable frictionless entry to other countries for people whose COVID immunisation and test records are held by HSCB and PHA, regardless of whether they are digitally enabled.
* Create a national approach that protects Health Services from being burdened with Requests for immunisation and test data.

The solution required to deliver the COVID Certification Service include the design of a digital and non-digital journey for users of the service, provision of the digital components of both journeys, and backend integration with existing immunisation and testing databases, which are the Vaccine Management System (VMS) held by HSCB and PHA and the Central Test Registry (CTR) held by the PHA. (In the future the CCS may interface with the CTR)

Both the digital and non-digital solutions will aim to align with the European Health Network interoperability standards for the Digital COVID Certificate and WHO Smart Vaccination Certificate data standards and architecture. It is also desirable that solutions adopted across the common travel area (CTA) are aligned and interoperable.

The infrastructure developed in support of the CCS, will also be utilised to support domestic use cases, to support regulations that will be in place.

The components to support this service are outlined in the process flow diagram (Figure 1.) that describe both international travel and domestic use cases flow.

All the components mentioned below make up the COVID Certification Service

* Citizen Web Application: An online portal journey to allow the public to:
  + Discover the CCS service
  + Registration for issuance of a COVID status certificate and providing supplementary information to support the certification
    - Capturing Health and Care Number (HCN) and optionally validating the number against the NIDA[[1]](#footnote-2) information
  + Processing the COVID status certification application
    - Indicate destination and date of travel helping prioritise requests
    - Issue ticket no for edge cases / manual transfer that allows follow up of issues in service support
    - Indicate preferred method of verification and have ergonomic path e.g. to book test
    - Matching and retrieval of immunisation and test data
    - Generate a digitally signed QR code containing retrieved data as per the technical specifications the service is to align with e.g. EU Digital COVID Certificate
    - Generate the Certificate with the QR Code imbedded in the required formats
      * PDF / Printable format for Offline access
  + Mechanism to request a new certificate
  + Send notifications via the Gov.UK gateway
* NIDA: Identity Verification and Authentication component managed by NICS
  + Provide citizen Identity authentication via NIDA service to LOA2 (Level of Assurance for validating user identity)
    - Users can create new accounts, uplift existing NIDA accounts
    - Incorporate an IA service to automate the Identity Assurance and verification within NIDA via SureCert. This will include incorporating IA in to the various LOA2 uplift scenarios and continuing to have a manual check as required where the automated check fails (?)
    - Logic to process the various SureCert outcomes including where a partial check is completed, and additional information is required to complete the check e.g. DOB
    - Cost Containment features to ensure the data sent to the SureCert API is valid. This will include the use of SDKs to capture ID documents and motion selfies
    - Mechanism for users to manage the NIDA account including resetting passwords and updating personal information which will feed into the CCS
* Citizen Mobile App: A certification mobile app that will:
  + Allow the user to login using the Identity authentication via NIDA
  + Download the digital certificate from the CCS Backend API(s) and store it on the Mobile App
  + Register destination and date of travel – receive country specific advice
  + Allow users to request a new certificate
  + Allow users to store the Digital App in the phone digital wallet
  + Allow users to register with NIDA if they don’t have an account.
* COVID Backend Services
  + Covid Pass API Gateway - API gateway to allow requests from Web application to be presented to the backend services for retrieval of data, checking and generating data against policies that determine a citizens COVID status, calculating status outputs and generating a QR Code that will be presented back to the citizen via the web application.
  + Status Calculator and QR Generator - components to carry out the validation and calculation of a citizens COVID status based off the data that it receives from the citizens vaccine and test results and assesses that data against policies from the policy engine that define the overall COVID status for the citizen before producing a QR containing Citizen and COVID status information
  + Matching Engine - The matching engine will provide a policy rules engine where the rules on how a Citizen is matched to records and a COVID status is calculated. These rules are defined by a policy maker(s) that are then used by the status calculator to determine the COVID status of the citizen.
* COVID Status Data Cache (CSDC)
  + Data cache to load and store a subset of the test and immunisation data surfaced from the CTR and VMS via ETL (Extract Transfer Load) process
  + Provide secure APIS to allow the COVID Service back services to match demographic users details to COVID records and retrieve COVID test and immunisation data for the purposes of generating a citizen COVID Certifications.
* Admin Portal / Call Centre Portal
  + Management portal to manage the policy and application configurations
  + Support non-digital requests for COVID Status Certificates
  + Provide a manual work queue to allow processing of COVID Certification requests which require manual intervention due to data quality issues / exception scenarios
  + Allow for a secure communication channel between citizens and DHCNI for any issues with the services e.g. via My Direct secure messaging.
  + Manage users of the system and the certificates issued by the system. Allows admin users to mark certificates as expired, invalid and manage user status
* COVID Match Service
  + Match a user’s profile to the data cache records based on the NIDA Demographic data
* COVID Status Calculator
  + Service to calculate an individual’s COVID status based on the data retrieved from the CSDC, including vaccine and test data
  + Service will contain the rules around issuing and expiry of QR codes created by the QR Code generator.
* Certificate DB
  + Data store for certificates generated by the COVID Certification Service to share with print services, web portal and mobile app.
* Integrations
  + HH GLOBAL: Send print files to the NHS Printer (HH Global Printing)
  + GOV.UK Notify: Send email & SMS notifications from the new COVID Certification Service.
* Monitoring and report
  + Provide a basic dashboard on the various service applications and services
  + Reporting and statistics on the use of the system e.g. number of users, number of QR codes issued, number of QR codes verified.
* CovidCert NI App: This is the end user mobile app, used by everyone who has requested a certificate.

There is also a separate COVIDCert Check NI App/Verifier App: This app allows a gate keeper/ verifier (gatekeeper/ verifier here refers to the person who checks the COVID status) to check the COVID status certificate is valid. There is a separate [DPIA](https://covid-19.hscni.net/covidcert-check-ni-mobile-app/) for the COVIDCert Check NI App and associated [guidance](https://covid-19.hscni.net/covidcert-check-ni-guidance-for-venues-event-organisers/) for gatekeepers/ verifiers.

# CCS Roles and Responsibilities

The Department of Health (DoH), Health and Social Care Board (HSCB) and Public Health Agency (PHA) are joint data controllers for the CCS. A Joint Controller CCS MoU has been agreed and signed, and a copy resides with each Data Controller.

All the data processors involved in the delivery of the CCS are appointed under UK GDPR compliant agreements and contracts, in compliance with Article 28 of the UK GDPR.

Appendix B sets out the arrangements for and the details of the Data Processors.

# Consultation & Stakeholders

The NI COVID Certification Service is being established under an Oversight Group chaired by the DoH Chief Medical Officer (CMO). The Steering Group, which reports to the CMO, is independently chaired by Dr Edward O’Neill with membership from DoH, PHA, and HSCB

Key stakeholders include:

* Department of Health
* Public Health Agency
* Health and Social Care Board
* Privacy Advisory Committee
* Information Commissioners Office
* Business Services Organisation – (IT)
* Belfast Health and Social Care Trust (BHSCT)
* Kainos – software development company
* Civica - software development company
* BigMotive – A user experience and software development company
* Department of Finance (DoF)- responsible for NIDA and NI Direct – call centre provider
* Political representatives
* Media

Due to the urgent requirement to establish and operationalise the service, a formal consultation was not undertaken. However, informal engagement is ongoing with a range of stakeholders.

DHCNI also remain in close contact with our counterparts in England, Scotland and Wales.

## **CCS Governance**

A CCS Product Team has been formed by DHCNI on behalf of the Department of Health to design, develop and co-ordinate the roll out of the CCS. This is headed up by Dr Edward O’Neill who acts as the Product Manager for all aspects of the COVID Certification Service.

The CCS Product Manager provides expert clinical advice and development prioritisation to the CCS development team product owners, one for Kainos the other for Civica. The CCS Product Manager works directly for COVID Certification Implementation Group. The CCS Product Manager, is tasked with, amongst other responsibilities, to ensure that the:

* CCS is used for its intended purpose
* CCS data processing is appropriately bounded in time and scope,
* This DPIA report is kept under review and up to date, and
* Co‐ordination of the necessary analysis to assess the efficacy of the CCS.

The CCS Product Manager, Product Owners and supporting development teams meet daily to ensure COVID Certificate Service priorities. The CCS Product Manager provides regular updates on the uptake and functioning of the CCS. Requirement prioritisation is conducted by the Product Manager who in turn directs CCS development through the Product Owners to the suppliers. Once the CCS moves to the strategic variant, day to day management of the system will move to BSO who will manage the system using standard ITIL change control, configuration, and service support processes.

# Data Processing Overview and Scope

This section of the document describes the CCS data that will be sourced, 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.

## **D**ata Subjects

The proposed data processing within the CCS relates to all citizens in NI who apply to receive a COVID Certificate through CCS.

## Purpose of processing

The CCS product has been developed by an existing DHCNI software partner Civica (data processor), on behalf of the joint controllers.

Citizen personal information will be used for the following purposes:

* **Civica** - process citizen data to perform a citizen data match to verify against the Vaccine Management System (VMS) and/ or Central Test Registry (CTR) records and process the certification generation request.
* **BigMotive** - provide user design service for the web application available for the applicants
* **Kainos** - process data as part of processing operations for the VMS and will provide the citizen vaccination data that is part of VMS, to be used by Civica in CCS to match against the user entered information.
* **Department of Finance** - who provide NIDA and NI Direct services- will process citizen data as part of the identity checking service they provide for citizens – ‘The NICS Identity Assurance service (NIDA)’. Use of NIDA along with the SureCert Service delivered by NI Direct provides a real-time ID and Biometric identity checking service, to enable citizens to prove their identity in order to access government services. This will be the first part of the process where an individual will add their identity details, which will be verified here and then sent to HSC data processors for the above matching and checks to be performed before a certificate is requested.
* **Ernst & Young (EY)** - will provide a temporary team to support HSCB staff in conducting manual matching where the CCS cannot do this automatically and to maintain the certificate generation volumes. EY will also provide a team for the COVIDCert call centre for citizens to apply for an exemption COVIDCert.
* **HH Global** - process citizen data in order to print hard copy certificates when required.
* **The HSC Regional Business Services Organisation (BSO)** will process testing data on behalf of the PHA, as they host the Central Test Registry (CTR), which stores the public testing (Polymerase Chain Reaction (PCR)) test results.
* **Belfast Health and Social Care Trust (BHSCT)** process citizen data as they host the CCS, VMS and CTR applications on their Microsoft Azure platform.

**Public Health Agency (PHA)** will review the processing of your exemption application should a citizen not agree with the **outcome.**

**Health and Social Care Board** will process a citizen’s exemption application in relation the administration of service payments to GPs.

**Trusts and GPs** are separate Data Controllers who will process a citizen’s exemption application, reviewing it in relation to medical records, to facilitate a citizen’s application. Their processing of a citizen’s data sits outside the CCS with the exception of the processing of the outcome of their review of a citizen’s application, which will be notified to CCS for the purposes of confirming whether or not a medical exemption certificate should be generated for a citizen by the CCS.

Further details regarding roles and responsibilities are available in Appendix B.

The information processed for CCS may be used by the Public Health Agency (PHA) for analysis for health research, health protection and health promotion purposes. Anonymised information may be used for reports and the production of official statistics.

# Context of Processing and Data Items Processed

If you use the CCS, data is collated in line with the eHealth Network JSON Technical specification guidelines for EU digital COVID certificates[[2]](#footnote-3). CCS can be used for travel and domestic purposes. If you use the COVID Certification Service and app to procure a certificate for travel, you will be asked to provide only the information we need to arrange that certificate for the desired date of travel.

The data collected by the CCS will include a citizen’s personal details and intended travel details. Personal details are collected to match a citizen’s details against the vaccination records included as part of the VMS, and/or test records as part of the CTR.

Personal details collected for domestic and international travel purposes include:

* Full Name
* Date of Birth
* Postcode
* Health and Care Number (HCN)
* Mobile Number
* Vaccination Centre (Optional; in case of other data mismatch)

For Domestic Vaccine Certificates

* Vaccination Centre (Optional; in case of other data mismatch)

For people intending to travel abroad internationally:

* Date of Travel
* Country of Travel

The above data will be used to check against personal data held in the VMS and shared with CCS for the purposes of vaccination certification. Personal data shared from the VMS to certify vaccination within the CCS will include the citizens:

* Number of doses
* Vaccination Date
* Vaccination Manufacturer
* Disease Targeted
* Vaccine Product
* Vaccine prophylaxis
* Vaccination batch
* Administering centre

Personal data shared from the CTR ,held by BSO, to certify recovery within the CCS will include the citizens:

* PCR test date and Test Type

An exemptions process for CovidCert is in place for citizens who qualify for an exemption certificate. Details of eligibility can be found on [NIDirect](http://www.nidirect.gov.uk/covid-exemption-certificate).

For CovidCert exemptions the following personal data will be collected during the exemption registration process:

* Health & Care Number (if available)
* Full Name
* Date of Birth
* Address

A table summarising how a citizen’s data us used and collected is shown below:



The COVID Certification Service (CCS) will never:

* Disclose any personal or health/medical information provided by a citizen to anyone other than a citizen’s GP practice patient record system.
* Ask a citizen to dial a premium rate number (for example, those starting 09 or 087) to speak to us.
* Ask a citizen to make any form of payment or purchase a product of any kind.
* Ask for any details about a citizen’s bank account.
* Ask for a citizen’s social media identities or login details, or those of a citizen’s contacts.
* Ask for any passwords or PINs, or ask a citizen to set up any passwords or PINs over the phone.
* Ask a citizen to download any software to their PC or ask a citizen to hand over control of their PC, smartphone or tablet to anyone else.
* Ask a citizen to access any website or smartphone application that does not belong to the Government, or HSC.

## Use of Data

Citizen data is used for the purpose of generation of COVID Certificates by the processes as described below:

1. **NIDA Authentication Process:**

The NICS Identity Assurance service will be used for User Identity Assurance Registration and Verification. The process is started when a user is requesting to open the COVID Certification Service client application. The citizen is required to have a LOA2 or higher permissions NIDA account which they require two factor authentication to login. The citizen is also required to have internet access during the login and registration process.

Once NIDA has authenticated the user, NIDA calls out to the Covid Certification Service to provide user information. This call is made to a known endpoint on CCS over a secure connection. Having completed the matching process, NIDA passes back to CCS with a signed token confirming the authentication of the user.

In order to perform the authentication process, NIDA service has been extended to:

1. Integrate with the SureCert AI Service to provide real-time ID and Biometric identity checking service
2. Implement SureCert AI Cost containment measures to avoid verification failures on the SureCert API including:
   1. Use MiTek SDK to capture ID document and Motion Selfie
   2. Service design of screens to capture and confirm Personal and Address information
   3. Classify the SureCert API failures which will be (1) returned to the user to resolve (2) Send to manual verification or (3) Reject the verification e.g. deceased user details
   4. Configurable number of ID and Biometric ID checks/Retries for users before being passed to manual verification process.
3. Support for manual verification of AI verification requests, which fail the SureCert biometric checks, based on certain failure conditions.
4. **COVID Matching Service:**

The CCS Data cache is periodically updated from an export of VMS. When the user has submitted their request for Covid certification, CCS matches the NIDA demographic details and HCN number against the immunisation and test data in the Data Cache.

When the user initiates a request for a COVID Certificate the flow will execute the match algorithm rules to identify a user’s records using the combination of personal details entered. HCN must be validated against the Patient records to ensure it’s a valid HCN/DOB combination before checking for COVID records.

1. **COVID Status Calculator Service**

A citizen should be able to request a COVID Status Certificate after authenticating via NIDA. The COVID Certificate can be used by the citizen to prove they are COVID safe for the purpose of travel or for access to domestic venues and events. This can be done by Providing a 3rd party (Verifier) with a scannable QR code.

The algorithm to calculate whether a citizen is eligible for a COVID Status Certificate or not is based on a set of rules, taking the citizens vaccination data and diagnostic test results into consideration. The rules are to be configurable through changes to the backend admin service.

The algorithm which will determine whether a citizen is eligible to be issued a COVID Status or not is based on a set of business rules, which will take the vaccination data, test results and antibody test results into consideration.

1. **2D Barcode Generation and Signing**

After the matching service successfully matches the users entered data to the VMS information and provides vaccination details for the certificate, the solution will use 2D Barcode (QR Codes) which is securely signed by the issuer to ensure its authenticity for the purposes of travel, or domestic uses.

* The 2D Barcode (QR Codes) is used to certify the COVID status of the user.
* The COVID status is validated by scanning the 2D Bar code which checks the signature on the 2D Barcode is valid and displays the details associated with the certificate.

A 2D bar code is only created if the data associated with the user complies with the business rules deciding whether a citizen is eligible for a safe COVID status or not.

The 2D barcode is generated within CCS using a self-signed certificate which is held securely within the CCS Production environment. The private key element of the certificate is accessed by the CCS backend to produce digitally signed QR codes. The public element of this certificate is publicly published for relevant solutions, such as the Verification apps of other UK nations, to use in the verification of NI-issued QR Codes. This public element has also been on-boarded with the EU Gateway via NHSx for use in verifier solutions across the EU via the EU Trust Gateway.

The Private Keys used for signing QR codes are securely stored in English Covid certification backend and only the signing service has access to it.

The UK Public Keys upload the EU Digital COVID Certificate Public Key Gateway Directory (PKD) which the visiting country scanner app can then use for verification.

The QR Code that is generated follows the EU standards as specified by the European Commission and can be found at <https://ec.europa.eu/health/ehealth/covid-19_en>)

1. **Certificate Delivery**

A citizen can retrieve their issued COVID Certificate with the 2D Barcode by requesting it to be delivered:

* Via a printed letter
* Digitally on a mobile App
* Digitally via the web App

The digital COVID Certificates can be accessed via internet access. The citizen will need to open the COVID Mobile or Web app and actively request their QR code if a valid certificate is not already stored on their device.

A typical scenario is that:

* The citizen requests a certificate via the COVID Status Service Web App
* The citizen receives an SMS, informing them when the COVID Certificate is available.
* The citizen opens the Web or Mobile app to retrieve their COVID Certificate(s).
* The app queries the backend to retrieve the COVID Certificate including the 2D Barcode.

Table 1. (below) provides details of the certificate entities across all the components of CCS Apps as mentioned above

|  |  |
| --- | --- |
| **Entities** | **Description** |
| My Certificates  (CovidCert NI app) | * The 2 types of certificates a user can have are –   + Domestic   + Travel * The user can see these certificates on My Certificates page in CovidCert NI app |
| Domestic Certificate QR Display  (CovidCert NI app) | * 2D Barcode Contains HSC defined pay load and Public key Encrypted payload. * 2D Barcode contains a security certificate and the code string identifier only – no personal or health data. * Photo –   + The selfie photo is sandboxed in the app and does not go anywhere.   + It has an alphanumeric code that is an identifier that is transmitted to the back end.   + The code cannot be reconstituted into any identifiable information.   + The verifier app does not read the photo. * Containing –   + User Reference as GUID   + Certificate Type, Digital or Paper   + Image Hash   + Security Code |
| Travel Certificate QR Display  (CovidCert NI app) | * Verify the security cert against the public key – reject invalid * Check expiry date not breached – reject expired * Check metadata and display name with verify message if valid * Prompt the user in verify message to check ID and visually check vaccination cert for dose 2 of 2 * The prompt will be ‘dynamic text’ that we can alter when Janssen one dose vaccine becomes available later this year, or we get a booster policy position * 2D Barcode contains the DCC standard:   [https://github.com/ehn-dcc-development/ehn-dcc-schema](about:blank)  [https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate\_json\_specification\_en.pdf](about:blank) |
| Domestic Certificate QR Scan  (CovidCheck NI app) | * Verifier timestamped code sent by CovidCert NI app. * Pass 2D Barcode payload to server for validation of vaccination status. * Response: Valid or Invalid (No additional data is show) * The verifier reads the security cert and verifies that – it also bounces the code off the backend * The health data is air gapped from the query coming in * On receipt of the code, the backend rules engine simply allows the verifier app to receive a piece of code to surface an accept or reject screen – no personal data, or health data is in that code – the rules engine is protecting the health data, acting as that air gap * Data shown to user in CovidCheck NI app is the First and Last Name within the DCC 2D Barcode payload * The verifier app does not store the notification code in surfacing the accept / reject notice * The notification auto clears within a number of seconds – no data is stored on the verifier app   Result Page shown for configured amount of time (initially 10 sec). |

Table 1. Certificate entities in CCS

# Compliance with data protection law and other regulatory guidance

**The UK GDPR Lawful Basis for Processing**

We process personal information according to the UK General Data Protection Regulation and the Data Protection Act 2018, which will be referred to as Data Protection legislation. Personal data is processed for CCS as part of our public task (in line with UK GDPR Article 6(1)(e))[[3]](#footnote-4).

The HSCB, PHA and Dept of Health statutory duty, is outlined in the Health and Social Care (Reform) Act (Northern Ireland) 2009, as below:

HSCB includes:

* The Regional Board shall exercise on behalf of the Department— (b)such other functions of the Department (including functions imposed under an order of any court) with respect to the administration of health and social care as the Department may direct.

DoH includes:

* Section 2(1) the duty to promote in Northern Ireland an integrated system of health care designed to secure improvement in the physical and mental health of people in Northern Ireland and in the prevention, diagnosis and treatment of illness, and
* Section 2(3)(g) the duty to secure the commissioning and development of programmes and initiatives conducive to the improvement of the health and social well-being of people in Northern Ireland, and
* Section 3(1)(b) the power to provide, or secure provision of, such health and social care as it considers appropriate for the purpose of discharging its duty under section 2; and do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of that duty.

PHA includes:

Providing strategic oversight and coordination of the implementation and ongoing delivery of regional vaccination programmes; provision of resources for health professionals and the public; interventions to improve uptake; disease and vaccine coverage surveillance; investigation, and management of cases, outbreaks and other immunisation incidents; and provision of expert advice to policy makers, commissioners, providers and the public.

In this instance the public task relates to the functions of the Public Health Agency which the Agency exercises on behalf of the Department of Health for:

* the health improvement functions mentioned in section 13 subsection (2);
* the health protection functions mentioned in section 13 subsection (3); and
* obtaining and analysis of data and other information in section 13 subsection (4).

Domestic use COVID certification regulations (The Health Protection (Coronavirus, Restrictions) Regulations (Northern Ireland) 2021) have been enacted in NI as a measure to mitigate the spread of COVID infection.

The COVID Certification Service supports a range of digital and non-digital services to enable citizens to evidence their COVID status to required standards (for the purpose of mitigating the rate of spread of COVID infection within NI, and as a result of international travel).

Some of the data processed relates to health data which is described as ‘special category data’. In relation to that processing, the following UK GDPR conditions apply:

* Article 9(2)(h) – the processing is necessary for medical diagnosis, the provision of health treatment and management of a health and social care system.
* Article 9(2)(i) – the processing is necessary for reasons of public interest in the area of public health.
* Article 9(2)(g) – the processing is necessary for reasons of substantial public interest.
* Data Protection Act 2018 Schedule 1, Part 1 (2) – Health or Social Care Purposes
* Data Protection Act 2018 – Schedule 1, Part 1 (3) – reasons of public interest in the area of public health
* Data Protection Act 2018 – Schedule 1, Part 2 (6) para (1) – for reasons of substantial public interest.

**Common Law Duty of Confidentiality**

Under common law, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider’s consent, (this can include implied consent). In practice, this means that all patient/client information, whether held on paper or computer, must not normally be disclosed without the consent of the patient/client. However, there are several very specific circumstances that makes the disclosure of confidential information lawful, including the sharing of necessary information with other health/care professionals and agencies where the interests of patient safety and public protection override the need for confidentiality.

The CCS team has engaged with the Privacy Advisory Committee (PAC) regarding the CCS secondary uses of data for CCS purposes and they are content that common law conditions for processing are met given the CCS has no secondary uses of data.

**Necessity and Proportionality**

In Northern Ireland, the COVID-19 Certificate Service has been mandated by the NI Executive, to enable NI citizens to travel internationally, by providing Covid Certificates, which meet EU and WHO standards and requirements. The NI Executive have also mandated the use of Covid Certificates in domestic settings and have instructed the Department of Health to implement Regulations to make this a statutory obligation for certain venues and events. A separate [DPIA](https://covid-19.hscni.net/covidcert-check-ni-mobile-app/) covers the policy and related Regulations for the introduction of Covid Status Certification in Domestic Settings in NI.

The optimal way to provide NI with a simple, easy and speedy COVID Certification for travel purposes and domestic use cases has been enabled by a single CCS. Only the minimum data set necessary is processed to enable citizen’s personal data and vaccine, or test, data matching for certificate generation.

COVID 19 is still a new and relatively unknown disease, and actions will be determined by both local (NI) experience of it as well as from wider national and international experience, knowledge and understanding. While it is recognised that specific actions may need to change, and may do so rapidly, as understanding and knowledge of the disease develops, the personal data collected through the CCS will only be used for purposes of generation of COVID Certificates for individuals who request them.

The DHCNI partnership, DoF- NI Direct and key suppliers have worked jointly on the development and delivery of a multi-channel COVID Certification Service (CCS) that has, by virtue of vaccination or COVID testing, facilitated international travel (meeting EU and WHO requirements). The CCS will also provide the necessary mechanism to enable certificates to be generated for domestic uses, to enable verifiers to scan the 2D barcode on domestic certificates for access to venues and events, in compliance with the Department’s Regulations- (further information about this processing is covered in the DPIAs for both the Verifier app and Introduction of Covid Status Certification in Domestic Settings, previously referenced and linked).

The CCS aims:

* To keep the process clear and simple for the public
* To reassure the public about the way their data is managed, and demonstrating alignment with ICO guidance on data minimisation and compliance with data protection legislation
* To securely verify the identity of individuals
* To comply with emerging and changing EU and WHO standards
* To assist Verifiers to comply with Regulatory requirements regarding access to venues and events in domestic settings.

The requirement to use the Covid Certification Service to provide evidence of your Covid status is currently required by most private sector organisations such as airlines, cruise ships and holiday operators to allow access to their services for international travel; similarly, for domestic use cases requirements have been put in place for:

* Indoor events (where some or all of the audience are not normally seated) with 500 or more attendees
* Outdoor events (where some or all of the audience are not normally seated) with 4,000 or more attendees
* events where more than 10,000 people will be present, regardless of whether or not they will be seated
* Nightclubs
* Licensed Hospitality premises and unlicensed premises for the duration of the time when they are operating under an occasional licence or when BYO alcohol is consumed
* Cinemas, theatres and conference halls

**CCS Data Retention**

Data for the CCS will be retained in line with GMGR section G43 Electronic Patient Clinical Records (inc Audit Trails)[[4]](#footnote-5) developed since 2013. Within the record keeping system, there must be a method of deciding ‘what is a record?’ and therefore ‘what needs to be kept?’ This is described as ‘declaring a record’. A declared record is managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.

We will only keep the record of a citizen being issued a travel vaccine certificate in the CSS for a maximum of 1 year after the date of travel. Domestic vaccines will be retained for 1 year after issue. A citizens vaccine record on the data cache is retained for a day. Data sent to the secure printers is retained for 30 days.

Retention will relate to operational records that need to be kept for legal compliance, or that have a limited life as part of an operational activity. These records will be retained for seven years (the current year plus six financial years). Records will not be kept after the retention period unless:

1. The record is the subject of live litigation or a request for information. In these circumstances, destruction should be delayed until the litigation is complete or the relevant complaint procedure has been exhausted, at which time a new trigger point and retention period is created.
2. The record has long-term value for the organisations statutory functions.
3. The record has been or should be selected for permanent preservation.

Any uploaded data recorded on Gov.UK Notify is held for seven days.

Any data shared between the CCS and other public healthcare systems will be protected under Data Sharing or Access Agreements between controllers and the relevant party and will include expected retention.

Processor Agreements/ Contracts and MoUs will also include instructions regarding retention periods and destruction of information held by processors.

**Data Rights**

The GDPR sets out the 8 rights that individuals have in respect of their data. These have been considered in respect of the NI COVID Certification as follows:

1. **The right to be informed**

Individuals are provided with information about the collection and use of their personal data for the CCS, including what personal data is collected, the purposes for collecting, retention periods and potential sharing of data, via the CCS Privacy Notice.

1. **Right of access**

Individuals can ask for copies of the information that we hold about them. Individuals can contact the respective DPO and contact details are provided in the Privacy Notice.

1. **Right to rectification**

Individuals can ask to have inaccurate personal data corrected or completed if it is incomplete. Individuals can contact the respective DPO as per the Privacy Notice.

1. **Right to erasure**

GDPR introduced a right for individuals to have personal data erased (‘the right to be forgotten’), however the right is not absolute and only applies in certain circumstances.

1. **Right to restrict processing**

Individuals have the right to request the restriction or suppression of their personal data, however the right is not absolute. While individuals can request that CCS stops processing their data, data will be held as set out in number ‘d’ above.

1. **Right to data portability**

Individuals can ask CCS to share their information with another organisation (although this may not always be possible).

1. **Right to object**

Individuals have the right to object to the processing of their personal data, including when the lawful basis for processing is public task. However, this is not an absolute right, and processing can continue if there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

1. **Rights relating to automated decision-making**

Individuals will not be subject to solely automated decisions which may have a legal or significant impact on their rights. CCS uses computer systems to process personal data for the purposes of matching of citizen records to the vaccination data and eligibility of COVID certificate based on the data on the number of doses received by the citizen (this is further elaborated in Sections 3 and 4 of this document).

However, app users can contact our helpline and progress their application manually if any issues are encountered. If users have any questions or concerns they can email [covidcertni@hscni.net](mailto:covidcertni@hscni.net).

**Prevention of CCS Scope/ Function Creep**

When citizen information is collected and processed for one reason but is then used or processed in ways beyond the original CCS purpose this is called function creep. Measures are in place to ensure this is prevented.

Any technical or functional changes needed to be made to the CCS require a formal request be made to the CCS programme team. These are then prioritised, costed and applied to a technical backlog for subsequent development.

Technical or functional changes that are needed to enable the sharing of CCS data with a 3rd party or additional government agency will require the development and approval of an appropriate Data Sharing or Access Agreement (DSA or DAA) and consultation with the controller DPOs. These can only be approved by the Personal Data Guardian (or equivalent) within the data controller organisation once usage has been determined to satisfy this DPIA, confidentiality and appropriateness. This may also require the data controller organisation to confer with invested stakeholder groups prior to approval being given. This formal process ensures there is clear accountability and governance of the CCS during development and on-going operation.

# Security Measures

Security measures are in place to ensure the information processed is carried out only as detailed in this DPIA and ultimately only for the purposes intended.

## CCS Information Security

The organisational and technical security measures implemented include the following:

* CCS citizen data can only be accessed under specific circumstance by authorised administration staff at GP practices, and Trusts.
* Trust, and GP practice staff are nominated access by their role within their area of business only. Users will not be able to use the system unless added to an application role.
* Access to citizen data is monitored by security and authentication mechanisms. Data access by CCS administrators and development staff is also monitored and recorded for audit purposes.
* All 3rd party access is in accordance to agreed contacts and contract management processes.
* An appropriate separation of roles is employed for all access granted.

## Security Controls in place for the CCS

All CCS Suppliers, as mentioned in Appendix B, comply with both international and industry-specific compliance standards and participate in rigorous third-party audits and penetration testing that verify security controls. As required by the UK GDPR, the CCS developers implement and maintain appropriate technical and organisational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data they process as data processors on its customers' behalf.

CCS administrators can run a report on any record to see all the staff who have accessed it, what if any change were made and where that access was appropriate or necessary.

Appendix D gives more detail about the CCS security measures in place.

## How we control users who has access to the CCS

The organisational security measures implemented include the following security controls that have applied to the environment:

1. Restriction on user access to the CCS
   1. Two factor authentication is used by Civica to control administration access for the web platform via mobile or email.
   2. All Azure resources are securely managed via Azure Active Directory. This provides a mechanism to ensure only those who are on the system directory and authorised can access the CCS.
   3. Connections to the CCS database[[5]](#footnote-6) are also encrypted via SSL/TLS and access is only granted via managed identity used by the Data Science CCS, reporting dashboard, and data extract processes. I.e., there is no direct access to the database via a user of the Azure portal
   4. All data stored in the Azure DB is strongly encrypted using industry standards[[6]](#footnote-7)
   5. Perhaps add something here about how all those who access CCS have been appropriately trained in the use of the system and in data protection.

# Identify and Assess Risks (what are the risks)

|  |  |  |
| --- | --- | --- |
| Describe source of the risk and nature of potential impact on individuals | | Likelihood of harm |
| **1** | **Access by nominated CCS programme staff and developers** to citizen data (held where) during product development cannot be limited, resulting in potential live data access to CCS developers (what potential impact might this have on individuals?) | Possible |
| **2** | **Risk of data loss during import of patient data from (which platform?) by Kainos** solution to the Civica CCS Data Cache resulting in low quality, low confidence population(?). This will reduce the ability to generate COVID certificates | Remote |
| **3** | **Risk of data breach** by staff working in the CCS Teams, through human error or intent.  Potential impact of damage or distress to individuals.), reputational loss/ financial loss due to UK GDPR fines for data controllers and/or processors | Remote |
| **4** | **Risk of the CCS being ‘hacked’, with the theft of personal identifiable data** (data breach), with the risk of distress or reputational damage to individuals. Or the system being compromised or inaccessible because of a cyber security incident therefore CCS being unable to operate with no certificate generation. In addition, the risk of reputational damage/financial damage due to fines, to the DoH, HSCB and DHCNI. | Possible |
| **5** | **Risk of unauthorised access to the personal data on the CCS,** resulting in a data breach with potential impact of dstress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB and DHCNI. Is this not the same as what is covered by 6? | Possible |
| **6** | **Risk of unauthorised access (internal or external) to the personal data** on the CCS Data Cache, CCS requesting platform, resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB and DHCNI. | Possible |
| **7** | **Risk relating to Adult Safeguarding Privacy concerns,** particularly regarding inappropriate access to current information on identity and location. Vulnerable people may be particularly concerned about the risk of identification or the disclosure of information.  Communication issues with vulnerable adults – issues with receiving/understanding information/instructions. If there are inadequate disclosure controls, there is an increase in the likelihood of information being shared inappropriately Not sure of relevance to CCS here? | Possible |
| **8** | **Risk of noncompliance with Controller data protection and information** governance policies and procedures which may result in accidental or deliberate misuse of sensitive personal data with potential of data protection requirements not being adhered to and for a data breach with the potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB and DHCNI. | Remote as above |
| **9** | **Risk of access to personal data by 3rd party processors which may result in accidental or deliberate use of sensitive personal information.** Potential impact of a data breach, with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB and DHCNI. How does this differ from earlier risks? | Remote as above |
| **10** | **Risk that personal data is used inappropriately for analytical purposes (? Not sure what this might mean in risk terms?. Inappropriate** sharing of personal data which could result in potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB and PHA. | Rare as above |
| **11** | **Risk of fraudsters sending similar looking messages with malicious intent.** Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the DoH, HSCB and PHA. | Likely |
| **12** | **Risk of fraudsters setting up a similar web booking front end** with malicious intent. Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the DoH, HSCB and PHA. | Possible |
| **13** | **Risk of the CCS failing or suffering technical malfunctions rendering the system inoperable.** The impact of the CCS suffering failure would slow or reduce the service’ ability to issue certificates | Possible |
| **14** | **Risk of inaccuracy of data in the certificates being generated due to incomplete and inaccurate data in VMS.** Resulting in individuals receiving certificates that do not reflect actual details, and/or certificate not generated due to data mismatch | Rare |

# Identify Measures to Reduce Risks

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Describe source of the risk and nature of potential impact on individuals | | Options to mitigate (treat) the risk | Effect on risk (Eliminated, Reduced, Accepted) | Residual harm (Low; medium; or high) | |
| **1** | **Access by nominated CCS programme staff and developers to patient data** during product development cannot be limited | HSCB have several controls in place contractually suppliers covered under contracts.  Patient data processing and confidentiality is described and enforced by Civica Limited’s contractual and call-off terms under the UK's G-Cloud 11 & 12 framework agreements.  Patient data and confidentiality is covered and enforced by Civica contractual and call-off terms under the UK's G-Cloud 12 framework agreement. Civica may process patient data as a data processor for the purposes of development. No patient identifiable info in Civica or Kainos pre-production environments Patient data and confidentiality is covered and enforced under the UK's G-Cloud 12 framework agreement.  As well as guidance is there any procedural guidance staff must follow, also are all staff trained in data protection | Reduced | Low | |
| **2** | **Risk of data loss during import of patient data from Kainos** solution to the Civica CCS Data Cache resulting in low quality, low confidence population. This will reduce the ability of the to generate COVID certificates | Automatic electronic import process is used to load the Kainos VMS patient data extract on the Civica CCS Data Cache | Eliminated | Low | |
| **3** | **Risk of data breach** (with the loss or unauthorised sharing of personal identifiable data, with potential impact of distress or reputational damage to individuals.), by staff working in the CCS Teams, through human error or intent. In addition, the risk of reputational damage to the HSCB, PHA and DoH. | All involved HSCNI staff in the CCS are required to complete the HSC information governance and IT Security e-learning module.   * NI Direct has been established as the primary contact centre for the Northern Ireland Civil Service (NICS), its agencies and the wider public sector. * Risk and management of breach of confidentiality covered in training, in line with contract requirements. * Staff are subject to regulatory Codes of Conduct e.g., NMC and GMC which include duties of confidentiality. * Confidentiality clauses in contracts of employment of staff and supporting developer/advisory suppliers. * Appropriate disciplinary action will be taken in the event of proven breach | Reduced | Low | |
| **4** | **Risk of the CCS being ‘hacked’, with the theft of personal identifiable data** (data breach), with the risk of distress or reputational damage to individuals. Or the system being compromised or inaccessible because of a cyber security incident therefore CCS being unable to operate with no certificate generation. In addition, the risk of reputational damage to the DoH, HSCB, PHA and DHCNI. | Civica and Kainos comply with both international and industry-specific compliance standards and participate in rigorous third-party audits and penetration testing that verify security controls. As required by the UK GDPR, the CCS developers implement and maintain appropriate technical and organisational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data it processes as a data processor or sub processor on its customers' behalf. Civica meet the requirements of ISO 9001:2015 and develop/deploy their software products on the GDS approved G-Cloud provider Google Cloud. Google Cloud are ISO-27001, 27017 and 27018 certified.  The CCS developers follow the UK Standard Contractual Clauses (data resides in secure cloud locations within the UK.  The Belfast Trust (BHSCT) have applied the following security controls:  ● Common data services is unavailable to everyone on WWW except for users within two Azure Active Directory groups  ● Multi-Factor authentication is required to access the CCS outside of BHSCT Trusted locations (BHSCT and BSO Networks).  ● Legacy authentication has been blocked for all users.  ● Users will not be able to use the system unless added to an application role.  ● Application roles have been set up to ensure a “least privileged” approach  Civica security protocols include:  ● Firewalls deny access by default  ● Security patches applied automatically  ● All external traffic in transit encrypted  ● SSL 2.0, 3.0, TLS 1.0, 1.1 are disabled, only TLS 1.2, 1.3 allowed  ● No patient identifiable info in pre-production environments | |  |  | | --- | --- | | Reduced | Medium | | Medium | |
| **5** | **Risk of unauthorised access to the personal data on the CCS,** resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB, PHA and DHCNI. | Civica and Kainos comply with both international and industry-specific compliance standards and participate in rigorous third-party audits and penetration testing that verify security controls. As required by the UK GDPR, the CCS developers implement and maintain appropriate technical and organisational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data it processes as a data processor or sub processor on its customers' behalf. Civica meet the requirements of ISO 9001:2015 and develop/deploy their software products on the GDS approved G-Cloud provider Google Cloud. Google Cloud are ISO27001, 27017 and 27018 certified.  The CCS developers follow the UK Standard Contractual Clauses (data resides in secure cloud locations within the UK). The Belfast Trust (BHSCT) & Civica have applied the following security controls: ● Common data services is unavailable to everyone on WWW except for users within two Azure Active Directory groups ● Multi-Factor authentication is required to access the CCS outside of BHSCT Trusted locations (BHSCT and BSO Networks). ●Once logged into CCS, user actions are logged in an audit trail which includes CREATE, VIEW, UPDATE events on patient details  ●Legacy authentication has been blocked for all users.  ● Users will not be able to use the system unless added to an application role. ● Application roles have been set up to ensure a “least privileged” approach  ● Only required accounts have been sync’d from on premise to Azure Active Directory via AD Connect.  Civica controls -Civica sessions to the infrastructure (SSH access) records login time and IP source  -Once logged into CCS, user actions are logged in an audit trail which includes CREATE, VIEW, UPDATE events on patient details -Access to reporting functionality that includes export is controlled via individual user permission group that has to be explicitly assigned to selected users -SSH access require short lived (12 hour) SSH certificates, meaning regular re-authentication is required with the identity provider -Remote access is controlled using industry standard methods (SSH keys, no passwords allowed, secure VPN, roles and permissions assigned per user) | Reduced | Low | |
| **6** | **Risk of unauthorised access (internal or external) to the personal data** on the CCS Data Cache, CCS requesting platform, resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB and DHCNI. | **Civica controls** -Civica sessions to the infrastructure (SSH access) records login time and IP source -Sessions to the admin portal are logged. There is auto logout functionality in place after session expires. -Once logged into CCS, user actions are logged in an audit trail which includes CREATE, VIEW, UPDATE events on patient details -Access to reporting functionality that includes export is controlled via individual user permission group that has to be explicitly assigned to selected users -SSH access require short lived (12 hour) SSH certificates, meaning regular re-authentication is required with the identity provider -Remote access is controlled using industry standard methods (SSH keys, no passwords allowed, secure VPN, roles and permissions assigned per user)  **Belfast Trust Controls** -All Belfast Trust Azure resources are managed via Azure Active Directory -Access to BHSCT Trust based CCS Servers, Containers and Virtual Machines are restricted to via encrypted connection through Azure Bastion. Connection to Bastion is via whitelisted IP addresses only. Only named Azure Active Directory identities can access the DSVMs via this secure connection  Security of CCS data as it moves from Kainos, into and within the CCS platform: - Data is securely transferred from Kainos to CCS via encrypted SSL/TLS connection using a secure Azure Logic App flow. A secure managed identity is used to connect the Logic App to Dynamics CRM which is associated with a least privilege security role granting the minimum permissions to update the CCS data model. -A named CRM service account with least privilege access is used in conjunction with a registered Azure Active Directory App to authenticate and authorise the data extract application when connecting to the Contact Tracing system to retrieve data for sync to the reporting database -This connection between the data extract application and Dynamics CRM web services is encrypted via SSL using TLS encryption - Any CCS data stored in Cosmos DB will be encrypted at rest by default using AES-256 encryption. | Reduced | Low | |
| **7** | **Risk relating to Adult Safeguarding Privacy concerns,** particularly regarding inappropriate access to current information on identity and location. Vulnerable people may be particularly concerned about the risk of identification or the disclosure of information. Communication issues with vulnerable adults – issues with receiving/understanding information/instructions. | Administration access to the CCS is controlled (as set out above), so no unauthorised personnel have access to the CCS. CCS development staff have access to the data on the CCS; they are bound by the existing controls and policies and professional regulatory Codes of Conduct. | Reduced | Low | |
| **8** | **Risk of noncompliance with HSCB, DOH and PHA data protection and information** governance policies and procedures which may result in accidental or deliberate misuse of sensitive personal data with potential of data protection requirements not being adhered to and for a data breach with the potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB and DHCNI. | Development of DPIA to identify risks & put appropriate measures in place; There is mandatory Information Governance and IT Security training for all DoH, HSCB and PHA staff. All staff have access to their organisation’s Information Governance policies and procedures. All are available on each organisations intranet site; All staff bound by NICS and HSCNI employment contracts are bound by professional regulatory Codes of Conduct Appropriate disciplinary action will be taken in the event of proven breach | Reduced | Low | |
| **9** | **Risk of access to personal data by 3rd party processors which may result in accidental or deliberate use of sensitive personal information.** Potential impact of a data breach, with potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB, PHA and DHCNI. | No live system access rights are allocated to 3rd parties. All 3rd party access is in accordance with agreed contracts and contract management processes. | Reduced | Low |
| **10** | **Risk that personal data is used inappropriately for analytical purposes. Inappropriate** sharing of personal data which could result in potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the DoH, HSCB, PHA and DHCNI. | Developers and advisory suppliers are bound by NDAs align with Controller’s Information Governance standards.  Access to the Kainos CCS capability will be controlled via user management and allocation of appropriate rights and levels (e.g., read/write at various levels based on authorised need) | Reduced | Low |
| **11** | **Risk of fraudsters sending similar looking messages with malicious intent**. Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the DoH, HSCB, PHA and DHCNI. | National Cyber Security Centre (NCSC) principle in place for usage of SMS to ensure that the SMS is as safe as possible | Maintained | Low | |
| **12** | **Risk of fraudsters setting up a similar web booking front end with malicious intent.** Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the DoH, HSCB, PHA and DHCNI. | There is a large amount of material available via website, apps etc to ensure the public are fully aware of what information will be required and why. | Reduced | Low | |
| **13** | **Risk of the CCS failing or suffering technical malfunctions rendering the system inoperable.** The impact of the CCS suffering failure would slow or reduce the service’s ability to issue certificates | In the event of a major failure or catastrophe, the system will receive the highest priority in terms of resources and measures to restore back to normal operation. | Reduced | Low | |
| **14** | **Risk of inaccuracy of data in the certificates being generated due to incomplete and inaccurate data in VMS.** Resulting in individuals receiving certificates that do not reflect actual details, and/or certificate not generated due to data mismatch | The CCS auto matching algorithm has been developed with multiple fuzzy matching logics to include multiple- levels of check to assure that correct user record is identified for certificate generation.  A manual fall-back is also in place for this matching services, where EY staff manually match records for each certificate request that has been generated but did not process via the auto matching algorithm | Reduced | Low | |

# Appendix A- CCS Stakeholder Landscape



## Appendix B - Data Processors

All data processors are appointed under Data Processors Agreements in compliance with Article 28 of the UK GDPR, either via UK GDPR compliant contracts, or MoUs.

Under the terms of these arrangements HSCB is the data controller responsible for assessing that all processors listed below, except DoF/ESS, are competent to process personal data in line with UK GDPR requirements. In taking the CCS forward HSCB progressed the necessary procurements with third party processors for the CCS and as a result HSCB is the holder of the contracts and therefore responsible for ensuring processors are competent to process personal data in line with UK GDPR requirements. DoH is responsible for assessing that DoF/ESS are competent to process data in line with UK GDPR requirements under these arrangements. This assessment will consider the nature of the processing and the risks to the data subjects.

Under Article 28(1) HSCB will ensure that only processors that can provide “sufficient guarantees” (in terms of its expert knowledge, resources, and reliability) to implement appropriate technical and organisational measures to ensure the processing complies with the UK GDPR and protects the rights of individuals. DoH will ensure the same in regard to DoF/ESS.

Contracts or Memorandum of Understanding (MoUs) will be in place to govern relationships with the data processors, which set out the obligations of each party and the data controllers’ obligations and rights regarding the data that is being processed. All contracts adhere to established BSO Procurement and Logistics Services (PaLs) processes and legal input provided by BSO Department of Legal Services (DLS).

All data processing takes place within the UK area and as such is subject to legislation in the form of the UK - General Data Protection Regulation (GDPR).

The following provides a list ofdata processors involved in delivery of the system.

* **Civica** is a system integrator organisation who were chosen to develop the end-to-end CCS platform and are regarded as a ~~sub-~~processor contracted by the HSCB. Civica will provide support on an ongoing basis to the CCS configuration for the duration of its operation, as part of their contract.
* **Kainos** will provide the citizen vaccination data that is part of VMS, to be used by Civica in CCS to match against the user entered information and process the COVID certificate request where applicable. Kainos are contracted by HSCB.
* **BigMotive** is a software development company who were chosen to develop the CCS user interface and are responsible for the configuration of the CCS webforms and are regarded as a ~~sub-~~processor contracted by HSCB. BigMotive will provide support for user experience (UX) design on an ongoing basis for the duration of the CCS operation, as part of their contract.
* **DoF - NI Direct/ NIDA** – NIdirect is the official government website for Northern Ireland citizens which is run by DoF ESS. NIdirect aims to make it easier to access government information and services. It does this by working closely with Northern Ireland departments and other public bodies to collate key information based on users' needs. **NICS Identity Assurance service (NIDA)** is a service provided by DoF ESS via NI Direct for the purposes of identity verification.This will be leveraged to integrate with the SureCert AI Service to provide real-time ID and Biometric identity checking service. DoH have a MoU in place with DoF/ ESS, which covers provision of these services.
* **Surecert i**s a biometric identity provider who use facial biometric techniques and photo capture processes to establish an individual’s identity compared to authorised documentation (passport or driving licence) they submit as part of the approval. HSCB have a two-year contract agreed with Surecert for the provision of CCS identity matching.
* **HH Global** – HH Global are a UK government approved (framework CCS RM6170) secure printing organisation who produce NI’s secure printed certificates. Certificate data is sent to HH Global over an encrypted transfer protocol. These certificates incorporate several secure elements around the QR code, bar code and print layouts. These are done in accordance with the Four Nation COVID Certificate letter spec (release 2). HSCB have a contract in place with HH Global for the provision of this service.
* **Ernst & Young** – EY are providing temporary data SME resources to support the call centre support, manual matching and edge case workload in support of HSCB staff. EY are contracted by HSCB via G-Cloud.
* **Business Services Organisation** (BSO) is a statutory organisation providing services as a data processor for HSCB and PHA. BSO are responsible for monitoring and managing all Microsoft contracts as commissioned and monitored by HSCB and PHA. They are responsible for all Civica environments user access and provision of new user hardware (PC and phones). BSO ITS are responsible for the supply and maintenance of user hardware. PHA and HSCB have overarching SLAs with the BSO for services including ITS. Their services are managed via appropriate agreements with PHA and HSCB.
* **Belfast Health and Social Care Trust (BHSCT).** BHSCT is a statutory organisation providing VMS, data exchange and CTR services as a processor for HSCB and PHA. BHSCT host the CCS, VMS and CTR applications separately on their Azure platform on individual instances. Their services are managed via appropriate verbal agreements with HSCB and PHA. A formalised MOU between the parties is being developed.

**Appendix C – Security Measures**

The solution will have the following layers of the security within the architecture

* **Authentication:** ensures that only authorized third parties will gain access to the system
  + The proposed identity service Azure AD has built in features that can help protect against threats to resources and data within the solution. Among these threats are denial-of-service attacks and password attacks.
  + Denial of service attacks can affect resource availability while password attacks can lead to unauthorised access to resources. It is critical that both are mitigated. Azure AD B2C defends against SYN flood attacks using a SYN cookie. Azure AD B2C also protects against denial-of-service attacks by using limits for rates and connections
* **Database encryption:** ensures that data is stored securely in the database
* **Firewall protection:** protects the solution from malicious attacks and ensures that all users will be able to access the solution by preventing overuse/misuse.
* **Secure virtual network (VNet):** ensures all backend services (API, DB and data ingestion) are located on a secure virtual network. Access to the VNet will only be possible through the API which is guarded by the firewall

A high-level threat model which identifies the data stores, processes, data flows and trust boundaries that exist in the platform has been created. This model is used to support the identification of necessary system security controls based on the proposed architecture.

The threat model takes the following into account for each system component and assesses them the STRIDE threat descriptions across the frontend, backend, and data cache.

* **Spoofing identity**. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.
* **Tampering with data**. Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.
* **Repudiation**. Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. **Nonrepudiation** refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.
* **Information disclosure**. Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.
* **Denial of service**. Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.
* **Elevation of privilege**. In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defences and become part of the trusted system itself, a dangerous situation indeed.

The CCS retains a full audit history of both user access (who viewed what and when) and an audit history on field-level record modifications. The later will record:

* The record that was changed,
* Who changed it,
* Timestamp,
* The value before the change,
* The value after the change for the affected fields.

The CCS developers follow the UK Standard Contractual Clauses (data resides in secure cloud locations within the UK). Civica and The Belfast Trust (BHSCT) have collectively applied the following security controls to protect the CCS:

* Multi-Factor authentication is required to access the CCS outside of BHSCT Trusted locations (BHSCT and BSO Networks). Legacy authentication has been blocked for all users.
* Common CCS data services are unavailable to everyone on WWW except for users within Active Directory groups
* CCS sessions to the infrastructure (SSH access) records login time and IP source to track users
* Access to reporting functionality that includes export is controlled via individual user permission group that must be explicitly assigned to selected Civica users
* Application roles have been set up to ensure a “least privileged” approach
* Only required accounts have been sync’d from on premise to Active Directory via AD Connect.

1. ‘The NICS Identity Assurance service (NIDA)’ is the identity checking service provided by Department of Finance [↑](#footnote-ref-2)
2. https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate\_json\_specification\_en.pdf [↑](#footnote-ref-3)
3. This refers to the processing that is necessary for the performance of the official tasks carried out in the public interest. [↑](#footnote-ref-4)
4. <https://www.health-ni.gov.uk/sites/default/files/publications/health/gmgr-disposal-schedule.pdf>, page 53 [↑](#footnote-ref-5)
5. Microsoft Azure DB [↑](#footnote-ref-6)
6. At rest by default using AES-256 encryption. [↑](#footnote-ref-7)