COVIDCert Check NI 'Verifier app'

DATA PROTECTION IMPACT ASSESSMENT

version 02, 27th Oct 2021

DPIA Ref no. *(Information Governance to provide)*	
Project Name	
COVIDCert Check NI 'Verifier app'	
Business Area	
DoH	
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);** **Steven Bergin (PHA)**	**Dr Edward O'Neill** **COVIDCert Check NI 'Verifier app' Solution Manager** **COVIDCert Check NI 'Verifier app'**

Contents

1. DPIA COVIDCert Check NI 'Verifier app'

This DPIA relates to the NI COVIDCert Check NI 'Verifier app'(COVIDCert Check NI 'Verifier app') and describes the process within Northern Ireland to verify COVID Certificates for all eligible certificate holders that can be used for the purpose of international travel and domestic use cases.
This DPIA is intended to cover processing activity by third party controllers as set out in Article 35(10) of UK GDPR.

2. Purpose of the COVIDCert Check NI 'Verifier app'

The Verifier app has been developed by the Department of Health (DoH) to enable 'Verifiers'[1] to certify a member of the public's Covid Status. It will be used by Verifiers, where the Northern Ireland Executive has decided that it is in the public interest to permit only those persons who possess evidence of, being fully vaccinated against COVID-19 to be present on the Verifier's premises to minimise as far as possible the risk of transmission of the virus which causes COVID-19.

This DPIA has been drafted in line with UK GDPR. Although personal data is not being processed by the Department of Health (DoH) in relation to this app, this DPIA has been drafted to ensure transparency and to maximise the public's confidence in the app.

Each Verifier who uses the NI Verifier app is required to have their own privacy notice and they should make these privacy notices available to the public. A template for these can be found on the ICO website - make your own privacy notice.

3. COVIDCert Check NI 'Verifier app'

Overview

The Verifier app has been developed by the Department of Health ('DOH', 'we', 'our') and DoH has overall responsibility for the functionality and delivery of the Verifier app. It will be delivered by Digital Health and Care NI (DHCNI) team on behalf of the DOH.

This DPIA applies to the NI Verifier app only. There is a separate DPIA that applies to the processing carried out as part of the Covid Certification Service (COVIDCert Check NI 'Verifier app') and related COVIDCert NI Cert App , which explains how your data is processed when you chose to use the Service to certify your Covid status.

[1] Verifiers' refers to the personnel appointed at venues who will verify/check COVID certificates using this app

The Department will not process any personal data in relation to the Verifier App. Users of the Verifier App will temporarily process your data for the purposes of verifying your Covid status (as explained below).

How does is work?

The NI Verifier app allows the Verifier to scan a COVID Pass 2D barcode, displayed by a member of the public from their Covid Certificate, either via the 2D barcode available on the COVIDCert Check NI app, or via a hard copy Covid Certificate, to show their COVID Pass status.

The scanning device for the 2D barcode is known as the NI Verifier app and is downloaded as an app to a mobile device from the Apple Play Store or Google Play in order to verify COVID certificates. Secure paper vaccination certificates can also be scanned by the NI Verifier app.

The NI Verifier app reads 2D barcodes that are presented to it and allows the Verifier to check the validity of the 2D barcode.

The scanner or verifier views the information contained in the 2D barcode by using the camera on the phone of NI Verifier operator. Once the 2D barcode is successfully scanned a number of results will be returned:

- For domestic use2, scanning a 2D barcode generated for domestic use and events using the NI Verifier app, will generate a green for a “valid” certification status or a red for “invalid” certification status screen. Citizens presenting a paper certificate for scanning will result in a yellow check screen on the Verifier App status screen. There is no further opportunity to see any further details as a result of that scan.

- For international travel, scanning a 2D barcode generated for travel use using the NI Verifier app, will generate a teal blue “valid” screen and request the user to check the citizen’s identification. A red “invalid for travel” screen will be shown if it doesn’t satisfy the NI vaccination travel rules.

In terms of architecture, the Verifier mobile scanner application utilises "Visual Studio App Centre" to log metrics of all different builds and versions of the scanner application. The anonymous analytics of app operation are securely sent to Azure App Insights. No personal data is processed.
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.

2 Domestic use refers to visiting domestic venues like bars, pubs, clubs, concert halls, stadiums etc.

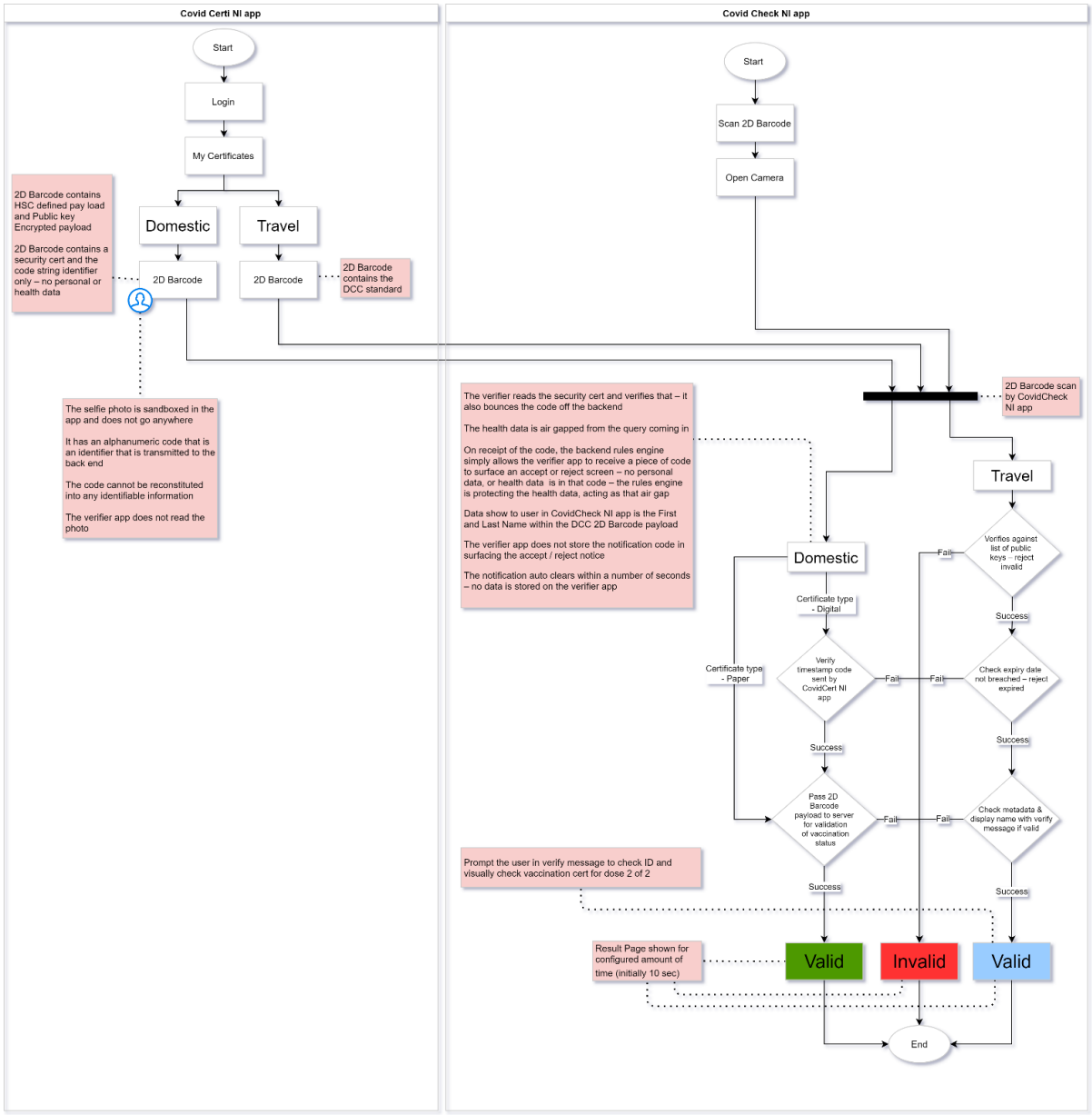

Figure 1. Process flow diagram

4. Consultation & Stakeholders

The NI COVIDCert Check NI 'Verifier app'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:

- The Northern Ireland public
- Venues and verifiers using this app

- Department of Health
- Public Health Agency
- Health and Social Care Board
- Privacy Advisory Committee
- Information Commissioners Office
- Belfast Health and Social Care Trust (BHSCT)
- Civica - software development company
- BigMotive – A user experience and software development company
- Political representatives
- Media

COVIDCert Check NI 'Verifier app' Governance

A COVIDCert Check NI 'Verifier app' 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 app. This is headed up by Dr Edward O'Neill who acts as the Product Manager for all aspects of the app. The Product Manager provides expert clinical advice and development prioritisation to the development team product owners. The COVIDCert Check NI 'Verifier app' Product Manager, is tasked with, amongst other responsibilities, to ensure that the:

- COVIDCert Check NI 'Verifier app' is used for its intended purpose
- COVIDCert Check NI 'Verifier app' 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 COVIDCert Check NI 'Verifier app'.

The COVIDCert Check NI 'Verifier app' Product Manager, Product Owners and supporting development teams meet daily to ensure priorities. The Product Manager provides regular updates on the uptake and functioning of the COVIDCert Check NI 'Verifier app'. Requirement prioritisation is conducted by the Product Manager who in turn directs the development through the Product Owners to the suppliers.

5. Data Processing Overview and Scope

This section of the document describes the COVIDCert Check NI 'Verifier app' 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.

Data Subjects

The proposed data processing within the COVIDCert Check NI 'Verifier app' relates to all citizens in NI who intend to visit a location where COVID certificates are verified through the COVIDCert Check NI 'Verifier app'.

Purpose of processing

The COVIDCert Check NI 'Verifier app' 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

6. Context of Processing and Data Items Processed

If you use the COVID Certification Service 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 will include your personal details and intended travel details. Personal details are collected to match your details against the vaccination records included as part of the VMS, and/ or test records as part of the CTR.

Personal details collected include:

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

Intended travel details (only for International Travel)

- Date of Travel
- Country of Travel

Use of Data

There is no use of personal data, as it is not transferred to the app, instead it just scanned from the certificate where this data is held encrypted within a 2D Barcode. This code is generated in the COVID Certificate by the COVID Certification Service (CCS) by the below process:

Within CCS, after the identity matching service successfully matches the users entered data to the vaccination information and provides vaccination details for the certificate, the solution will generated 2D Barcode (QR Codes) which is securely signed by the issuer to ensure its authenticity for the purposes of travel.

- 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 Solution uses the NHSD Devolved Administrations and Crown Dependencies Citizens QR Generator.
The reason the solution will use the NHSD service is:

- It is the UK which controls borders for all constituent countries part of the United Kingdom. For this reason, internationally recognizable and verifiable Covid Status QR codes should be signed by a central UK authority.
- The UK will be responsible for on-boarding with EU Trust Gateway. This approach avoids Northern Ireland having to negotiate with the EU to get onboarded to the EU Trust Gateway.

The QR code digitally signed by the NHSD QR code generator service with the private key for the UK is sent to the COVID Status application for the Devolved Administration or Crown Dependency. When the travel or event administrator (which could be a Gatekeeper, Steward or Border Official) scans the QR code in the COVID Status application or another EU DGC compliant scanner, the signature is verified using the associated UK public key – this way we can ensure that the COVID status QR code is valid and was issued by UK QR code generator solution or associated DA. 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 2D Bar 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)

Table 1. (below) provides details of the certificate entities across all the components of COVID Certification Service Apps (both COVIDCert App and COVIDCert Check Verifier App), in reference with Figure 1:

Entities	Description
My Certificates (CovidCert NI app)	▪ The 2 types of certificates a user can have are – o Domestic o 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 – o The selfie photo is sandboxed in the app and does not go anywhere. o It has an alphanumeric code that is an identifier that is transmitted to the back end. o The code cannot be reconstituted into any identifiable information. o The verifier app does not read the photo. ▪ Containing – o User Reference as GUID o Certificate Type, Digital or Paper o Image Hash o 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 https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_json_specification_en.pdf

Domestic Certificate QR Scan (CovidCheck NI verifier 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. Verification entities in COVIDCert Check NI 'Verifier app'

7. 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 COVIDCert Check NI 'Verifier app' as part of our public task (in line with UK GDPR Article 6(1)(e))[3].

In line with the HSCB and Dept of Health statutory duty, as stated in the Health and Social Care (Reform) Act (Northern Ireland) 2009, which sets out the functions of the HSCB, including that:

- 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.

[3] This refers to the processing that is necessary for the performance of the official tasks carried out in the public interest.

And DoH which include:

- 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.

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 1 (4)** – reasons of public interest in the area of public health research
- **Data Protection Act 2018 – Schedule 1, Part 2 (6) para (1)** – for reasons of substantial public interest.

Necessity and Proportionality

Civica has been commissioned by DoH to develop the COVIDCert Check Verifier App, and is part of the suite of applications in support of the COVID Certification Service.

Necessity:
This processing is required to comply with the law regarding access to premises. There is a need to be able to verify an individual's COVID status and check they have: been fully vaccinated against COVID-19 for international travel, and or domestic purposes. There must

be assurance that the COVID certificate provided by an individual has been issued from an authorised party.

Proportionality:
A digital app solution is able to do this securely and quickly using complex algorithms to verify digital certificates embedded into the 2D bar codes being scanned. Automated checking is more accurate than humans reading long strings of random characters and numbers. No personal data is stored or transmitted by the App.
The provision of a centrally developed and secure app limits the likelihood for third party apps with different privacy controls. Therefore it has been determined that it is better for a centralised body to provide a digital app rather than rely on the market to produce various different apps, or require venues (particularly smaller ones) to create their own system.
The COVIDCert Check NI 'Verifier app' 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.

COVIDCert Check NI 'Verifier app' Data Retention

No personal data is collected or stored via this solution. App usage metrics data is sent from the App to the Civica staff to view and analyse the metric data. The metrics data is in aggregated format - no personal identifiable data is shared
The personal data displayed within the Verifier App is deleted at the point the Verifier returns/begins another scan

Data Rights

As no data is stored within the Verifier App, data rights are not applicable here.

Prevention of COVIDCert Check NI 'Verifier app' Scope/ Function Creep

When citizen information is collected and processed for one reason but is then used or processed in ways beyond the original COVIDCert Check NI 'Verifier app' 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 COVIDCert Check NI 'Verifier app' require a formal request be made to the COVIDCert Check NI 'Verifier app' 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 COVIDCert Check NI 'Verifier app' 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 COVIDCert Check NI 'Verifier app' during development and on-going operation.

8. 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.

COVIDCert Check NI 'Verifier app' Information Security

- No personal data / information is stored in the app. The encrypted 2D bar code is scanned for the purpose of verification. Hence no personal data is accessible by any user or developer of the app

Security Controls in place for the COVIDCert Check NI 'Verifier app'

COVIDCert Check NI 'Verifier app' suppliers 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 COVIDCert Check NI 'Verifier app' 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. COVIDCert Check NI 'Verifier app' 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.

9. Identify and Assess Risks (what are the risks)

Verifier

The following table identifies the risks for who download and use the app for its defined purpose on behalf of their employer i.e. verifying that an individual's COVID certificate has been issued by a trusted authority.

Risk	There is a risk the app user copies the personal data displayed to them either by writing it down or taken a screen shot in order to steal the personal data of the individuals who QR codes they are scanning.	
Impact	Loss of confidentiality to the individual whose QR code is scanned. There would be no health impact on the individual.	
Notes	This would be deemed misuse of the App for the purposes of data theft	
Unmitigated risk score	*Mitigation controls*	*Residual risk score*

Likelihood	4	The screen shot functionality has been disabled within the App. Limited personal data displayed – name and date of birth – which limits the possibility of identity theft. Organisations who expect their employees to use the App should remind their staff about handling of personal and sensitive data. However, it is recognised that this is outwith Civica control to enforce.	Likelihood	2
Impact	2		Impact	2
Score	8		Score	4

Risk		There is a risk that the app user scans QR codes that are not COVID status related.		
Impact		There is no impact on the individual whose non-COVID status QR code is scanned.		
Notes		It is thought that this is very unlikely to occur.		
Unmitigated risk score		*Mitigation controls*	*Residual risk score*	
Likelihood	1	The App is designed to read only QR codes that relate to an individual's COVID status. It can only decode QR codes using public keys issued by trusted authorities that were created for this purpose and no other. The public keys are retrieved from a store under Northern Ireland management and therefore meets Northern Ireland security standards.	Likelihood	1
Impact	1		Impact	1
Score	1		Score	1

System Developer and Operator

The following table identifies the key risks for Civica software engineers who will be developing the App.

Risk	There is a risk that the engineers share their user accounts.
Impact	Logs record all activity undertaken against the logged in account. If a concern is raised, then there is no way to distinguish between which user took which actions other than the honesty of the engineers involved. There would be no health impact on the individual.
Notes	Can't see this happening especially as working from home is currently the norm so less likely to use an already logged in device.

Unmitigated risk score		*Mitigation controls*	*Residual risk score*	
Likelihood	2	Each engineer has their own network login. Employment terms and conditions have been signed by the engineers. Engineers abide by the Civica Information Security Acceptable Use Policy. Engineers have all done the Civica IG training. Engineers user accounts will be removed if their role no longer requires access or they leave Civica employment.	Likelihood	1
Impact	1		Impact	1
Score	2		Score	1

Risk		There is a risk that the engineers misuse their privileged access to add malicious code, viruses, etc.		
Impact		Depends on the nature of the code introduced but could lead to poor performance, corruption of data, etc. leading to failure of the App to verify a QR code or being able to display the relevant details to the App user which could lead to an individual being denied access to services. There would be no health impact on the individual.		
Notes		Not expected to happen but potential exists		
Unmitigated risk score		*Mitigation controls*	*Residual risk score*	
Likelihood	2	Minimise the number of Civica staff with access to the CovidCert Verifier App environment. User accounts are provided with least privileges to carry out the tasks. Audit actions. Employment terms and conditions have been signed by the engineers. Engineers abide by the Civica Information Security Acceptable Use Policy. Engineers user accounts will be removed if their role no longer requires access or they leave Civica employment. Google and Apple review all versions of the App prior to allowing it to be made available for download in the app stores.	Likelihood	1
Impact	4		Impact	4
Score	8		Score	4

Risk		There is a risk that the software versions used to develop the App are not kept up to date or patched leaving vulnerabilities that can be exploited by bad actors.			
Impact		Depends on the nature of the vulnerability but most likely to lead to data theft due to decoded data in the App being able to be read by a bad actor. Loss of confidentiality to the individual whose QR code is scanned. There would be no health impact on the individual.			
Notes		The potential does exist			
Unmitigated risk score		*Mitigation controls*		*Residual risk score*	
Likelihood	2	Civica policies and procedures for software development and testing include checks for vulnerabilities. Independent penetration test carried out to check App for vulnerabilities. Google and Apple review all versions of the App prior to allowing it to be made available for download in the app stores.		Likelihood	1
Impact	4			Impact	4
Score	8			Score	4

Risk		There is a risk that a maintenance error exposes more data from the decoded QR code than is required for the app user to verify the validity of the QR code and the individual's COVID status.			
Impact		Loss of confidentiality to the individual whose QR code is scanned. There would be no health impact on the individual.			
Notes		The potential exists			
Unmitigated risk score		*Mitigation controls*		*Residual risk score*	
Likelihood	3	Change control procedures in place. Testing of any change prior to making a new version of the App available to users.		Likelihood	2
Impact	4			Impact	4
Score	12			Score	8

Risk	There is a risk that engineers misuse their privileged access to introduce code into the App that sends the data read from the QR code to another location effectively stealing the data.
Impact	Loss of confidentiality to the individual whose QR code is scanned. There would be no health impact on the individual. There would be no impact on the individual for access to the service as the data would still be displayed within the App to the user.

Notes		Not expected to happen but potential exists		
Unmitigated risk score		*Mitigation controls*	*Residual risk score*	
Likelihood	2	Limited personal data displayed – name and date of birth – which limits the possibility of identity theft. Minimise the number of Civica staff with access to the CovidCert Verifier App environment. User accounts are provided with least privileges to carry out the tasks. Audit actions. Employment terms and conditions have been signed by the engineers. Engineers abide by the Civica Information Security Acceptable Use Policy. Engineers user accounts will be removed if their role no longer requires access or they leave Civica employment. Google and Apple review all versions of the App prior to allowing it to be made available for download in the app stores.	Likelihood	2
Impact	4		Impact	4
Score	8		Score	8

Bad actors

The following table identifies the key risks for Unauthorised User Group; this group includes 'script kiddies', organised crime groups and hostile state actors.

Risk		There is a risk that a bad actor gains access to authorised user credentials via a phishing attack or other method.		
Impact		Depends on the account privileges that the bad actor gains access to but could lead to ransomware attack on Civica. There would be no health impact on the individual.		
Notes		In this risk, an authorised user is a Civica developer with access to the environment where the app is developed. Bad actors likely to try this but given that no personal or other data is held by Civica for this App it would be of little value to a bad actor to attempt this other than to disrupt Civica activity in general.		
Unmitigated risk score		*Mitigation controls*	*Residual risk score*	
Likelihood	3	No personal identifiable or other data is held by	Likelihood	2

Impact	4	Civica so there is no data to steal in relation to this App. Ensure Civica user accounts are given the minimum privileges needed to develop the app. Civica staff involved in the development and maintenance of the App have had training to be on the lookout for suspicious emails and not to open attachments they are not expecting.	Impact	4
Score	12		Score	8

Risk		There is a risk that the app is removed from either app store.		
Impact		Prevents individuals from downloading and using the app limiting its effectiveness. Possibly impacts on venues being able to verify individuals COVID status prior to entry.		
Notes		Can't provide the service to new users; existing users unaffected; should be resolved relatively quickly. There would be no health impact on the individual.		
Unmitigated risk score		*Mitigation controls*	*Residual risk score*	
Likelihood	3	Minimise store users with elevated permissions. Force MFA on all store users. Ensure tight processes on adding and removing users. Google and Apple have well developed processes in place to mitigate against this.	Likelihood	2
Impact	2		Impact	2
Score	6		Score	4

Risk		There is a risk that the app is replaced with a malicious app.		
Impact		Depends on what the malicious app does but could lead to theft of personal data as the unauthorised app contains code to copy the personal and other data to another location.		
Notes		The potential exists.		
Unmitigated risk score		*Mitigation controls*	*Residual risk score*	
Likelihood	2	Minimise store users with elevated permissions. Force MFA on all store users. Ensure tight processes on adding and removing users. Google and Apple have well developed processes in place to mitigate against this.	Likelihood	1
Impact	4		Impact	3
Score	8		Score	3

Risk		There is a risk that if a bad actor gains access, they can introduce malicious code, viruses, etc			
Impact		Depends on the nature of the code introduced but could lead to poor performance, corruption of data, etc. leading to failure of the App to verify a QR code or being able to display the relevant details to the App user which could lead to an individual being denied access to services. There would be no health impact on the individual. Individual may not be able to access venue.			
Notes		Without mitigation this is likely to be attempted.			
Unmitigated risk score		*Mitigation controls*		*Residual risk score*	
Likelihood	3	Minimise the number of Civica staff with access to the CovidCert Verifier App environment. User accounts are provided with least privileges to carry out the tasks. Audit actions. Google and Apple review all versions of the App prior to allowing it to be made available for download in the app stores.		Likelihood	2
Impact	4			Impact	4
Score	12			Score	8

Risk		There is a risk that a bad actor gains access to introduce code into the App that sends the data read from the QR code to another location effectively stealing the data			
Impact		Loss of confidentiality to the individual whose QR code is scanned. There would be no health impact on the individual. There would be no impact on the individual for access to the service as the data would still be displayed within the App to the user.			
Notes		This is possible but if the bad actor has gained access to the environment where the App is developed then there are more destructive things they can do such as create a ransomware attack on Civica.			
Unmitigated risk score		*Mitigation controls*		*Residual risk score*	
Likelihood	3	Limited personal data displayed – name and date of birth – which limits the possibility of identity theft. Google and Apple review all versions of the App prior to allowing it to be made available for download in the app stores.		Likelihood	2
Impact	4			Impact	4
Score	12			Score	8

<table>
<tr><td colspan="2">Risk</td><td colspan="3">There is a risk that unauthorised users could gain privileged access due to an unattended, unlocked device (i.e. developer’s laptop) (this risk is not related to app users’ mobile phone devices)</td></tr>
<tr><td colspan="2">Impact</td><td colspan="3">The impact depends on whose device the unauthorised user is able to access e.g. if it was an administrator account then deletion of parts of the App development environment might be feasible; or a user with normal access may allow the introduction of malicious code or viruses.
The impact also depends on the knowledge and skill level of the unauthorised user. They may have little knowledge of information technology beyond web browsing and online shopping or they may be a ‘at home technical wizard’.</td></tr>
<tr><td colspan="2">Notes</td><td colspan="3">Under current conditions where most people are working from home, the biggest threat will come from a family member.</td></tr>
<tr><td colspan="2">Unmitigated risk score</td><td>Mitigation controls</td><td colspan="2">Residual risk score</td></tr>
<tr><td>Likelihood</td><td>2</td><td rowspan="4">Civica engineers to lock screens when away from their device for any reason even if only for a short time.
All staff to be aware of their organisation’s policies for home working and information security.
Minimise the number of staff with access to deploy the App.
All user accounts created with the minimum amount of privileges but still allows staff to do their job.</td><td>Likelihood</td><td>2</td></tr>
<tr><td>Impact</td><td>3</td><td>Impact</td><td>3</td></tr>
<tr><td>Score</td><td>6</td><td>Score</td><td>6</td></tr>
</table>

Technical

The following table identifies the key risks due to technical issues

Risk	There is a risk that there is a technical outage (mobile device network) preventing the Apps being able to scan and verify a QR
Impact	There would be no health impact on the individual. The individual whose QR code is being attempted to be scanned for access to the service could be denied access if there is a mobile phone network outage.

Notes		All technical environments are subject to some risk failure.		
Unmitigated risk score		*Mitigation controls*	*Residual risk score*	
Likelihood	3	The App is designed to store the public keys for decrypting a QR code on the mobile device of the app user for a period of time preventing the need for a network connection to complete the verification process. Scanning of a QR code does not require an active mobile network.	Likelihood	1
Impact	3		Impact	3
Score	9		Score	3

Appendix A - 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 COVIDCert Check NI 'Verifier app' forward HSCB progressed the necessary procurements with third party processors for the COVIDCert Check NI 'Verifier app' 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 of data processors involved in delivery of the system.

- **Civica** is a system integrator organisation who were chosen to develop the end-to-end COVIDCert Check NI 'Verifier app' platform and are regarded as a ~~sub-~~processor contracted by the HSCB. Civica will provide support on an ongoing basis to the COVIDCert Check NI 'Verifier app' configuration for the duration of its operation, as part of their contract.

- **BigMotive** is a software development company who were chosen to develop the COVIDCert Check NI 'Verifier app' user interface and are responsible for the configuration of the COVIDCert Check NI 'Verifier app' 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 COVIDCert Check NI 'Verifier app' operation, as part of their contract.

- **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 COVIDCert Check NI 'Verifier app', 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.