MyCare

Users of the MyCare.scot Web application for

Initial Release in December 2025

Data Protection Impact Assessment V1.0

Healthier Scotland
Scottish Government

NHS SCOTLAND

MyCare

Table of Contents

Contents

Healthier Scotland Scottish Government NHS SCOTLAND

1. Key Information

Title of Project/Product	MyCare.scot Web Application
Reference No.	NESDPIA1035
Version control	V1.0
Date approved	27/11/2025
Owner	Digital Front Door (DFD) Programme – Delivery Board
Completed by	DFD Information Governance & Assurance Workstream
Information Governance Lead	DFD Data Protection Lead

2. Revision History

Version	Date	Summary of Changes
V0.1	26/09/2025	Initial drafting completed, including removal of all mentions of the term "app" for MyCare as per comms guidance. Several queries still outstanding, final checking and further changes before MVP go-live required due to ongoing live aspects of the programme.
V0.2	28/10/25	Updates based on comments from peer review & further clarifications from service teams/programme. Update term MyCare to MyCare.scot as per latest comms guidance. Included aspects around support, reporting and analytics.
V0.3	04/11/25	Updated contents page to accurately reflect page numbering and the document's content.
V0.4	21/11/25	Updates based on feedback from DFD Delivery Board and other sources..
V1.0	27/11/25	As approved by the DFD Delivery Board.

3. Glossary

Term	Explanation
Personal Data	is information that relates to a specific individual.
Special Category Personal Data	is personal data that needs more protection because it is sensitive. This includes data about your health.
Processed	data is "processed" when any action is taken with it. For example, when it is collected, transferred or deleted
Controller	an organisation or person that makes decisions about what, how and why personal data is processed. They are legally responsible for the data.
Processor	an organisation or person which processes personal data on behalf of a Controller and under specific instruction.

4. What are you trying to do and why?

High level description of your service/product:

MyCare.scot is a web-based application where users can interact more effectively with health and care services.

MyCare.scot is a digital platform accessible by adults in Scotland using a unique identifier, which contains personalised health and care information in a reliable, understandable format from services which are scheduled to, or already have, given them care.

MyCare.scot will provide users a secure method to digitally access information and services relating to their health and social care. The initial release in December 2025 will show only certain healthcare information for patients registered in NHS Lanarkshire, but will grow in future to include more health and social care services and be available to the wider population in Scotland. The services available in the initial release do not replace any existing services but will provide users the option to access certain information digitally.

The term Digital Front Door (DFD) is the name given to the wider project that includes developing the MyCare.scot online service.

The Scottish Government have published a document that provides a high-level summary of the vision and mission of MyCare.scot.

Aim, scope and purpose:

Overall Aim & Purpose

MyCare.scot is designed to provide a secure digital means for individuals to access information and services relating to their care. The web application itself will not store information about users but rather link in with other services or data sources in order to display information or provide functionality to users.

To do this, the Digital Front Door Programme will utilise existing public sector infrastructure or create new avenues where required, to enable MyCare.scot to connect to the required information in order to then show this to users within the application.

How MyCare.scot will Work

MyCare.scot is a cloud-hosted web application. The way it will interact with other services will be by using application programming interfaces (API) with each of the relevant systems. APIs are mechanisms that allow two software systems to communicate with each other using a specific set of rules. In effect, they allow two systems to "talk" to each other, but only in the specific ways that are built into each API design. Each API is set up to require specific pieces of information to be provided so it can then "talk" to the other system and provide the desired response. The process is often referred to as a "call" to an API or an API request and response. In this case MyCare.scot will "call" APIs and then display the responses to users.

A good example to illustrate the process is with weather apps:

- The weather data will be held in a central system, for example by the Met Office.
- The weather app will "call" to that system using an API and request the data relating to a specific area.
- The central system will provide a response back through the API to the weather app, providing only the data for that area.
- The weather app will then display the relevant weather for that area to the user.

So MyCare.scot will call the APIs for the relevant systems in order to make the information available to the user. For example, when a user wishes to see their vaccination history, they will:

- log in to MyCare.scot and navigate to the section showing vaccination data by clicking on the relevant section in MyCare.scot
- when the user clicks on that section, that will initiate MyCare.scot to call the API linked to the system that holds vaccination records.
- the call to the API will include the unique identifier for that user and the response to MyCare.scot will include only the records for that individual.
- MyCare.scot will display this information to the user.

By utilising APIs, MyCare.scot will be able to add new services and expand its functionality in future. The above example is a slightly simplified version and does not include the relevant steps around 'Identity/Access Tokens' which are explained further below.

Scope of Release

MyCare.scot will be available nationally in 2026. However, the initial release in December 2025 will be limited to individuals selected by NHS Lanarkshire that are residents registered with a GP practice in the NHS Lanarkshire area and are aged 16 or over. There will be an element of a phased release, meaning it is available to a smaller number of people on day one, with that number growing regularly. Details of any phased release will be agreed between NHS Lanarkshire and NHS Education for Scotland to ensure the online service and relevant systems are working properly.

Scope of Functions

MyCare.scot will release in December 2025 with functionality allowing users to view certain aspects of their health care information. This will grow in future to include social care aspects and further services. The Digital Front Door Programme will work with the relevant health and care organisations to create a relevant schedule for the new aspects.

For the December 2025 release, the following functionality will be available within MyCare.scot:

- Users will be able to securely sign-up and login to use MyCare.scot, after verifying their identity.
- Users will be able to see the following information relating to their care:
    - Demographic information, such as name, date of birth and address
    - Flu and Covid Vaccination records.
    - Allergies and medications
    - Secondary Care dermatology appointments details
    - Digital communications – messages sent from organisations providing care to users to a new secure digital mailbox.
- Users will also be able to search a directory of health and wellbeing services, including GP practices, dental services and support groups. This aspect does not include the use of personal data but is included for completeness.

Relevant Stages of Using MyCare.scot

ScotAccount – For sign-up and sign in

ScotAccount is a secure online service run by the Scottish Government, which allows users to sign in and verify their information for a variety of different services, of which MyCare.scot is one.

In order to access MyCare.scot, users will need to sign in using ScotAccount. On initial sign-up, users will have to verify their identity, or share previously saved identity data, through their ScotAccount. It is essential that identity verification is undertaken before providing access to highly sensitive information about someone's care. Once an individual has verified their identity in ScotAccount, they have the option to share the verified details with MyCare.scot which is necessary to use the service.

CHI Database & NDP Account Linking Service – to identify a specific individual

A Community Health Index (CHI) number, is a unique number given to every individual registered with a GP practice in Scotland. It was initially created for healthcare purposes in NHS Scotland, but is intended to roll out in Local Authorities for use within the social work and social care sector to. There is a central CHI Database held and managed within NHS Scotland.

With regards to the Digital Front Door Programme, once an individual signs in to their ScotAccount and agrees to share their verified information (first name, middle name, surname, date of birth and full address including postcode), the next steps are:

- These details are securely transmitted to the 'NDP Account Linking Service.' This service is one of the support services managed by NHS Education for Scotland that MyCare.scot makes use of.
- The NDP Account Linking Service use the verified details (first name, surname, date of birth and postcode) to search the national CHI Database to find that individual's CHI number.
- When a match is found, the CHI number is stored in a database known as the 'NDP User Store' held by the NDP Account Linking Service. This database stores an individual's ScotAccount ID along with their CHI number.
- After the initial sign-up process, when a user logs in, MyCare.scot will make use of 'tokens' to perform the different functions available, which are described in the next section.

Identity/Access Tokens – used for all functions of MyCare.scot

Identity/Access Tokens (referred to as 'Tokens' from here on) are time-limited parcels of information which MyCare.scot uses when performing all its functions. They are used to determine what users can access and include details about that person which are then used to determine what data should be retrieved through any API calls.

How Tokens are Used for MyCare.scot:

- After initial sign-up, when a user signs in to MyCare.scot through their ScotAccount login, the NDP User Store is checked to retrieve the necessary details and create Tokens that are passed to and stored by MyCare.scot
- When a user tries to do anything within MyCare.scot, it will:
  - check there are existing valid Tokens stored by MyCare.scot.
  - use the details from the Token to call the APIs of the other systems. Usually, the CHI number or ScotAccount ID are used so the API will provide only the information relating to that person in the response.
- If the Tokens have expired, then MyCare.scot will request new tokens from the relevant systems. This happens in the background and users are not required to do anything.
- If for some reason a user's account has been suspended or they have had their access to MyCare.scot blocked, then tokens will not be provided and that user will no longer be able to access MyCare.scot. This will only happen in instances where access has been specifically removed.

Retrieving Data – Calling APIs to display health and care information

The sections of MyCare.scot which display health and care information work as described above, using tokens and APIs to display information about the individual user.

For example, when a user wishes to view appointments data:

- The user will click on the appointment data section within MyCare.scot.
- MyCare.scot will first check for valid tokens.

- MyCare.scot will then use the CHI number included in these tokens and then call the appointments API by sending that CHI number.
- The API communicates with the system that holds appointments data, identify the relevant data for that CHI number and then provide the response through the API to MyCare.scot.
- MyCare.scot will then display the appointments data received to the user.

This process will be the same for most health and care services available through MyCare.scot.

ScotAccount Mailbox – for Digital Communications

The Scottish Government have created a secure digital mailbox for individuals to receive messages from public sector organisations. As part of the wider Digital Front Door Programme, this mailbox is being used to enable Scottish residents to receive digital communications relating to their care, with the initial example being secondary care dermatology appointment letters.

The ScotAccount Mailbox also provides the functionality to send people notifications when they receive a new message; either SMS text message, email or both. In the December 2025 release of MyCare.scot, the Digital Front Door Programme will use the ScotAccount Mailbox functionality to send notifications.

With regards to MyCare.scot: using APIs, MyCare.scot will have an icon displaying how many unread messages there are in the ScotAccount Mailbox. When the user navigates to the messages section of MyCare.scot, their messages from the mailbox will be displayed in MyCare.scot. Only messages relating to their care will be shown in MyCare.scot. Any messages in the ScotAccount Mailbox from other public sector services will not be available to view through MyCare.scot. The APIs used for the mailbox will transmit the ScotAccount ID number from the tokens (not the CHI number), as this is the identifying number used for the mailbox system.

As soon as an individual first signs up to use MyCare.scot, any service that can send digital messages (for example, secondary care dermatology appointments) will begin sending these messages to the user's ScotAccount Mailbox.

December 2025 – Eligibility List

For the initial release in December 2025, there will be a phased release meaning that a smaller number of individuals will have access on the first day, with that number growing each week.

The NDP Account Linking Service will be provided with a list of CHI numbers by NHS Lanarkshire for people eligible to access MyCare.scot. During the original sign-up process, once a user's CHI number has been found, this CHI number will be checked to see whether it is on the eligibility list. If the user is eligible, then the CHI number will be stored in the NDP User Store as described above and the user will be able to access MyCare.scot.

If a user is not eligible then their details will not be stored in the NDP User Store and they will not be able to access MyCare.scot. They will instead be directed to a web page with details as to why this might be the case and further information. This will also include individuals from Health Board areas other than NHS Lanarkshire who try to access MyCare.scot. They will be CHI-matched, found to not be on the list of eligible individuals and directed to the same web page providing information why this might be the case.

National Contact Centre - Support

If users are having difficulty with any aspect of MyCare.scot, they can contact the National Contact Centre (NCC), managed by National Services Scotland (NSS). The NCC will provide assistance to users and attempt to solve any issues they are having. If there are technical problems, then the NCC can raise the issue with the technical teams in NES and SG on behalf of the user. Depending on the type of issue, the NCC may have to signpost the user to contact another service directly but will provide clear details to the user of how they do that.

Reporting and Analytics

In order to understand how people are using MyCare.scot, an analytics provider called Plausible Analytics has been contracted to provide some usage and analytics data to the Digital Front Door Programme. This information is never used to track an individual, but rather better understand overall trends and patterns so we can improve the service in future. When users click on any web pages within MyCare.scot, an event about this web page is created and these events are sent securely to Plausible Analytics. These events include details of the device including IP address, browser and device type. Plausible Analytics use the IP address to look up country/region/city information and then immediately pseudonymise the data and never store the IP address itself. They use the pseudonymised number to understand which web pages of MyCare.scot that user has visited and whether they have visited several times in the same day. After each day, the method used to create the pseudonymised number is deleted so the data becomes fully anonymous. So if the same user used MyCare.scot the next day, there is no way to link their activities from other days.

Processing activity type:

Processing Activity 1: Provision of Healthcare Systems - Patient

Processing Activity 2: Provision of Software/Products and Services

Processing Activity 3: Reporting/Statistics

What is the driver for this project/service? *Provide context including if applicable, commissioning details, any supporting national policy or legislation.*
Scottish Government and COSLA's joint Digital Health and Social Care Strategy committed to people having greater access to their health and care data. MyCare.scot is an important step in the strategy's commitment to a 'Digital First' approach.

5. What personal identifiable information will be collected and used?

Categories of personal data:

Personal Data from ScotAccount – Used for CHI Matching			
Categories of individuals (data subjects)	Categories of personal data	Special categories of personal data	Sources of personal data
Users	Verified data items (after confirming identity through ScotAccount process) are shared: • First Name • Middle Name • Surname • Date of Birth • Full Address, including Postcode • ScotAccount ID Number Data items used for CHI Matching:	n/a	ScotAccount

	• First Name • Surname • Date of Birth • Postcode		

Data From Vaccination Records			
Categories of individuals (data subjects)	Categories of personal data	Special categories of personal data	Sources of personal data
Users	n/a	• CHI Number • Product name • Vaccination Date • Dose • Location	National Clinical Datastore, managed by NHS Education for Scotland and made available to MyCare.scot through APIs.

Data From the CHI Database – CHI Number & Demographics Information			
Categories of individuals (data subjects)	Categories of personal data	Special categories of personal data	Sources of personal data
Users	• First Name • Surname • Date of Birth • Address • Health Board	• CHI Number	National CHI Database, managed by National Services Scotland and made available to MyCare.scot through APIs.

Data From Emergency Care Summary System			
Categories of individuals (data subjects)	Categories of personal data	Special categories of personal data	Sources of personal data
Users	n/a	• CHI Number **Allergies** • Allergy description • Comments • Date recorded	Data originally created in GP practice systems, then centralised into the national Emergency Care Summary system, managed by National Services Scotland, and made

		Medications • Name • Dosage • Date prescribed • Date dispensed • Prescribed by	available to MyCare.scot through APIs.

Data Relating to Appointments			
Categories of individuals (data subjects)	Categories of personal data	Special categories of personal data	Sources of personal data
Users	n/a	• CHI Number Details of the Appointment, including: • Date/time • Location • Appointment Status • Details of who the appointment is with, such as a Consultant's name • Department / Specialty • Attached documents, such as appointment letters	Created in the Health Board's local patient administration system, and then passed to the support services in the National Digital Platform (managed by NHS Education for Scotland) which makes the data available to MyCare.scot through APIs.
Clinical Workforce	• First Name • Surname • Clinical Specialty		Included in the data relating to appointments. Created in the Health Board's local patient administration system, and then passed to the support services in the National Digital Platform (managed by NHS Education for Scotland) which makes the data available to MyCare.scot through APIs.

Data Relating to Digital Communications			
Categories of individuals (data subjects)	Categories of personal data	Special categories of personal data	Sources of personal data
Users	• First Name • Surname • Address • Email Address • Phone Number • ScotAccount ID Number	• CHI Number Details will depend on the type of message, but will include specifics around an individual's care. For example, appointment messages will include all the details relating to that appointment, including the attached appointment letter.	This information is originally created in the organisation providing you care (for example, Health Board or Local Authority) and then passed to the support services in the National Digital Platform (managed by NHS Education for Scotland) who format the data into the required message format and then pass to the ScotAccount Mailbox, managed by the Scottish Government. MyCare.scot requests this data from the mailbox using APIs.
Clinical Workforce	• First Name • Surname • Clinical Specialty		Names of staff providing care included in digital messages. This information is originally created in the organisation providing you care (for example, Health Board or Local Authority) and then passed to the support services in the National Digital Platform (managed by NHS Education for Scotland) who format the data into the required message format and then pass to the ScotAccount Mailbox, managed by the Scottish Government. MyCare.scot requests this data from the mailbox using APIs.

Data Relating to Support Services			
Categories of individuals (data subjects)	Categories of personal data	Special categories of personal data	Sources of personal data
Users who contact the National Contact Centre with issues	Depending on the nature of the call, some of the data that may be collected is: • First Name • Surname • Date of Birth • Address • Postcode • Email Address • Phone Number • ScotAccount ID Number	Depending on the nature of the issue, some of the data may be collected is: • CHI Number • Diagnosed Conditions • Prescriptions / medications • Other details relating to their healthcare and the issue they are having with MyCare.scot	This information will be mainly supplied by the user when they contact the National Contact Centre at National Services Scotland (NSS). NSS staff have access to the National CHI Database if necessary. NSS staff may also contact support services on the user's behalf.

Reporting & Analytics			
Categories of individuals (data subjects)	Categories of personal data	Special categories of personal data	Sources of personal data
Users of MyCare.scot	• IP Address of device used Other data items used but are not personal data, for example: • Device operating system • Browser used • Device type Plausible Analytics then use IP address to look up: • Country / region/ city	n/a	When someone use the MyCare.scot service, each time they click on any page it triggers something called an HTTP request. This request is collected by the analytics provider, Plausible Analytics.

Necessity and Proportionality

Necessity refers to the requirement that processing personal data must be strictly necessary for the purpose for which it is collected. It means that the processing operations, the type of data processed, and the duration of data retention should be essential and not unnecessarily broad or extensive.

Proportionality means that data processing, including limitation on data subjects' rights, should not go beyond what is necessary to achieve a legitimate objective. It requires a balance between the interests of the individual and the interests of the controller or processor. In essence it is about ensuring that data processing is justified, limited to what is necessary, and does not unduly infringe on the rights of individuals.

Explain how the data to be collected and processed is necessary for the specific purpose and is not simply convenient or optional, and that the processing is done in the least intrusive way to achieve your objective. Include any options appraisals that may have been undertaken.
Verifying an Individual's Identity & Locating their CHI Number In order to ensure that individuals access the right information, it is necessary to ensure we can verify their identity and locate their CHI number from the central system. ScotAccount is used for verification aspects, then it is necessary for the data items of first name, surname, date of birth and postcode to be used in order to accurately determine an individual's CHI number. **Personal Data displayed in MyCare.scot** The information relating to an individual's care that is displayed in MyCare.scot has been agreed by the organisations responsible for providing your care. The data displayed in MyCare.scot is only requested using APIs when a user either logs in or navigates to the relevant section, and is not stored long term or used for other purposes in MyCare.scot.

Describe how the personal data will be:

Collected:	For the December 2025 release, MyCare.scot will not collect data from users directly, but link to services where data has already been collected. **ScotAccount** During the process of creating a ScotAccount, users will supply the relevant details required. When a user verifies their identity using the

	ScotAccount process they can then choose to share these verified details with MyCare.scot. **CHI Database** The CHI Database is a central database that holds the details of all individuals in Scotland registered with a GP practice. The details are originally collected when that individual registers with their GP practice. **NDP User Store** The NDP Account Linking Service is one of the support services run by NHS Education for Scotland that MyCare.scot uses, and it stores the CHI number linked to the ScotAccount ID. These are collected in that service when the user attempts to log in to use MyCare.scot and a successful CHI match is made. **Identity/Access Tokens** These tokens are created by services used to support MyCare.scot, using the data from the three sections above: ScotAccount, CHI Database and NDP User Store, and then stored by MyCare.scot. **Vaccination Records** This data is initially collected when you receive a vaccination and is stored in the National Clinical Datastore, managed by NHS Education for Scotland **Emergency Care Summary (ECS) Data** The Emergency Care Summary is a summary of basic information about your health which might be important if you need urgent medical care when your GP is closed, or when you go to an accident and emergency department. This information is copied from your GP's computer system into a national database. MyCare.scot will show information about medications and bad reactions. **Appointments Data** Your Health Board will create appointments on their local patient administration systems. Some examples of when this happens is when they receive a referral from your GP, after you attended a previous appointment or other situations. This data is then transferred into one of the National Digital Platform support services managed by NHS Education for Scotland. MyCare.scot will call an API to this support service to then show appointments data within MyCare.scot.

	Digital Communications As part of the wider Digital Front Door Programme, new services have been put in place to enable digital messages to be sent to a secure mailbox managed by the Scottish Government. Messages created by health and care services will be transferred into this secure mailbox. MyCare.scot will then use APIs with the mailbox to display these messages. **Service Finder** This is Scotland's Service Directory and includes details of health and wellbeing services in Scotland, including GP practices, dental services and support groups. It does not include personal data. **December 2025 Release – Eligibility Lists** NHS Lanarkshire will provide the NDP Account Linking Service – managed by NES - with a list of CHI numbers for users who are eligible to use MyCare.scot. **Support Services – National Contact Centre (NCC)** When a user contacts the NCC, most of the personal data used to assist them with their issue is collected directly from the user. Other data may be collected from the systems that NCC staff have access to in order to provide support. **Reporting & Analytics Data** When someone uses the MyCare.scot service, each time they click on any page it creates an event which then sends an HTTP request. These requests are collected by the analytics provider, Plausible Analytics.
Transferred:	**Application Programming Interfaces (APIs)** Different APIs MyCare.scot uses have been built using different technologies. But all are secure methods to transfer data. **December 2025 – Eligibility List** These details will be sent using secure NHS Scotland email services between NHS Lanarkshire and NHS Education for Scotland **Support Services – National Contact Centre (NCC)**

	Most of the data will be provided verbally over the phone. The NCC may transfer details securely to the technical support teams using secure service desk systems. **Reporting and Analytics** The data is transferred using secure https and is encrypted in transit.
Accessed and Used:	**Users Accessing MyCare.scot** The data will stay in the relevant systems until a user starts using MyCare.scot. When users navigate to the different sections, MyCare.scot will call the corresponding API for that area and display the data. **Data Caching** When users access MyCare.scot, it will utilise APIs in order to show the relevant data to the user. In most instances, the responses from these APIs will be stored in something called a cache. A cache is somewhere to store data that MyCare.scot can quickly retrieve it from. This way, MyCare.scot does not have to repeatedly call external APIs but can show the data held in the cache a lot quicker. It also puts less strain on the health and care systems where that data is stored by reducing the number of API calls it has to respond to. Data is only held in the cache for 15 minutes and then removed, and data in the cache is stored securely. But caching the data allows MyCare.scot to run more smoothly for most uses. The only API calls that do not cache the responses are: the digital messages in the ScotAccount Mailbox and the results shown from Service Finder. Identity/Access Tokens are also stored in the cache. **Identity/Access Tokens** Whenever MyCare.scot attempts to do anything, it will first check whether there are valid tokens. If not, then it will request new token(s) from the relevant National Digital Platform support service. The details within the tokens are then used to call the different APIs in order to provide the desired response. E.g. CHI number used to request vaccinations information for that individual.

	<u>Support Services – National Contact Centre (NCC)</u> The personal data collected by the NCC will be used to try to resolve the issue the user has. This may also be provided to technical teams where they may need to look at technical issues a user is facing. **<u>Reporting and Analytics</u>** The data used by Plausible Analytics is anonymised within 24 hours and only used to provide anonymous statistics to help understand how people use the service.
Kept up to date, if necessary:	As data is not stored long term in MyCare.scot, there is no data that it must keep up to date. It is the responsibility of the systems that provide the data to ensure that the data is kept up to date where necessary. But by linking in with existing health and care systems, MyCare.scot will always show the latest data available. **<u>Support Services – National Contact Centre (NCC)</u>** NCC staff will record the details of the issue and the outcome. Once the call has been closed, there is no need for this data to be updated. **<u>Reporting and Analytics</u>** There is no requirement for this data to be kept up to date as it relates to an activity that occurred at a point in time.
Transferred outside of the United Kingdom: *Will personal data be transferred outside of the United Kingdom or countries without a European Commissioned designated adequate level of protection.*	MyCare.scot and the healthcare systems it interacts with do not transfer data relating to your healthcare outside of the UK as part of this work. The ScotAccount Mailbox uses contractors who store data in the UK and European Economic Area, which is covered under the EU-UK Data Adequacy Agreement. **<u>Reporting and Analytics</u>** To understand how people are using MyCare.scot, an analytics company called Plausible Analytics has been contracted to be able to provide analytics and intelligence in this area. The IP address of the user's device is used with Plausible Analytics whose services are in Germany. However, Plausible Analytics

	immediately pseudonymise the data and never store the IP address. This data is then anonymized after 24 hours.

Lawful basis and legal statues:

Lawful basis

There must be a valid lawful basis in order to process data. There are six lawful bases for processing – which is most appropriate will depend on the purpose and relationship with the individual whose data you intend to process. Most of the lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you will not have a lawful basis.

Article 6 Lawful Basis
6(1)(e) – It is necessary for the performance of a task carried out in the public interest
What is the legal gateway:
Details of organisation different roles are explained in the section below. For December 2025 release, NHS Lanarkshire will be Controller for all data processed within MyCare.scot. NHS Lanarkshire's legal gateway is their obligations to provide health and social care services under the National Health Service (Scotland) Act 1978.

If you are processing special category data, you also need to identify a special category condition for processing.

Special category data is personal data that needs more protection because it is sensitive. Special category data is defined as:

- personal data revealing **racial or ethnic origin**
- personal data revealing **political opinions**
- personal data revealing **religious or philosophical beliefs**
- personal data revealing **trade union membership**
- **genetic data**

- **biometric data** (where used for identification purposes)
- data concerning **health**
- data concerning a person's **sex life**, and
- data concerning a person's **sexual orientation**

Article 9 Lawful Basis (Special Category Data)
9(2)(h) – Health or social care (with a lawful basis in law)

Legal Status

The UK GDPR draws a distinction between a 'controller' and a 'processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. The UK GDPR defines these terms:

- **'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the process of personal data.

  Controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.

- **'joint controller(s)'** is where two or more controllers jointly determine the purposes and means of the processing.

  Joint controllers decide the purposes and the means of processing together – they have the same or shared purposes. Controllers will not be joint controllers if they are processing the same data for different purposes.

- **'processor'** means a natural level person, public authority, agency or other body which processes personal data on behalf of the controller.

  Processors act on behalf of the relevant controller and under their authority. In doing so they serve the controller's interests rather than their own. Although a processor may make its own day-to-day operational decisions, they should only process personal data in line with a controller's instructions, unless it is required to do otherwise by law.

What is NHS Education for Scotland (NES) role:

This high-level public-facing Data Protection Impact Assessment has been provided to inform users and the public of how MyCare.scot works.

More detailed assessments have been conducted by the relevant organisations involved in the Digital Front Door Programme to ensure the appropriate levels of due diligence have been carried out.

For MyCare.scot, NHS Education for Scotland act as a Processor to the organisations responsible for health and care services users receive.

December 2025 release

For the initial release of MyCare.scot, NHS Lanarkshire will contract NHS Education for Scotland to act as a Processor, meaning they will act at the instruction of NHS Lanarkshire.

In instances where non-NHS Lanarkshire residents attempt to access MyCare.scot, NHS Education for Scotland will be acting as a Processor to the relevant Health Board for the purposes of CHI-matching and checking the CHI number against the eligibility list. The user will not be on the eligible list, therefore not able to access MyCare.scot. For situations where an individual has been given access to MyCare.scot in NHS Lanarkshire and moves to another Health Board before the national roll-out, NES will be acting as a Processor to the new Health Board for some services and NHS Lanarkshire for the appointments and digital communications aspects.

Other parties' data roles:

NHS Lanarkshire

Controller of the health data being shown for their registered patients. NHS Lanarkshire contract NHS Education for Scotland to act on their behalf (as a Processor).

Remaining 13 NHS Scotland Health Boards

For instances where:

- an individual from a Health Board other than NHS Lanarkshire attempts to access MyCare.scot, the relevant Health Board that individual is registered to will be Controller for the purposes of using the verified details from ScotAccount to identify an individual's CHI number, check it against the eligible list and determine they are not eligible to access MyCare.scot.

- individuals who are given access to MyCare.scot in NHS Lanarkshire as part of the December 2025 release and move to another Health Board area before MyCare.scot is available nationally. These individuals will continue to be able to access MyCare.scot, with the new Health Board being Controller of the personal data processed in MyCare.scot except for digital communications and appointments that relate to NHS Lanarkshire services (where NHS Lanarkshire will continue as Controller).

The remaining 13 Health Boards are:

- NHS Ayrshire and Arran
- NHS Borders
- NHS Dumfries and Galloway
- NHS Fife
- NHS Forth Valley
- NHS Grampian
- NHS Greater Glasgow & Clyde
- NHS Highland
- NHS Lothian
- NHS Orkney
- NHS Shetland
- NHS Tayside
- NHS Western Isles

Scottish Government – ScotAccount
The ScotAccount service is managed by the Scottish Government, who act as the Controller for the data used within ScotAccount, up until a user agrees to share their verified details out with ScotAccount.

Scottish Government – ScotAccount Mailbox
The Scottish Government are Controller for the data held in the ScotAccount Mailbox, including messages originating from health and care. If the messages are viewed in MyCare.scot, then the organisation the message originated from will be Controller for the data that is shown through MyCare.scot, with NES acting as their Processor. For the December 2025 release this will be NHSL Lanarkshire. Scottish Government will remain Controller for the messages held in the ScotAccount Mailbox

National Services Scotland – National Contact Centre
National Services Scotland manage the National Contact Centre who users will be able to contact if they are having issues with the MyCare.scot service. National Services Scotland provide this service on behalf of the organisation responsible for providing health and care. So for the December 2025 release, that will be NHS Lanarkshire.

Plausible Analytics
Acting as a sub-Processor to NES for the very limited processing of personal data occurring with regards to reporting and analytics purposes.

This list is not an exhaustive list of all the organisations involved. Further organisations may be contracted by the above-listed parties as a Processor or Sub-processor.

6. Are there any risky aspects to this project

	High Risk Activity	Description
☒	**Innovative technology**	processing involving the use of innovative technologies, or the novel application of existing technologies (including AI).
☒	**Denial of service**	decisions about an individual's access to a product, service, opportunity or benefit that is based on any extent on automated decision-making (including profiling) or involves the processing of special category data.
☐	**Large-scale profiling**	any profiling of individuals on a large scale.
☐	**Biometrics**	any processing of biometric data.
☐	**Genetic data**	any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.
☒	**Data Matching**	combing, comparing or matching personal data obtained from multiple sources.
☐	**Invisible processing**	processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers the compliance with Article 14 would prove impossible or involve disproportionate effort.
☐	**Tracking**	processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
☒	**Targeting of children or vulnerable individuals**	the use of personal data of children/young persons (under the age of 18) or other vulnerable individuals.
☐	**Risk of physical harm**	where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

7. What are the benefits to this processing

What are the perceived benefits of this activity?
• MyCare.scot is a new service which offers people secure online access to their health and social care information in one place. • MyCare.scot gives people more choice and access to their information, so they can actively manage their health and care when, where and how they want. • MyCare.scot brings care closer to home, joining up services and tackling inequity. • We are co-designing MyCare.scot with users, ensuring that existing non-digital options are still available. • MyCare.scot will help with missed appointments, which will reduce waiting times for care and treatment. • The December launch is the first version of MyCare.scot, and as it evolves it will be able to do much more, with feedback from users.

8. Harm

What are the types of harm that could impact an individual because of the processing or in the event of a data breach?

	Category	Description & Examples
☐	**Financial harm**	Negligently, knowing, or purposefully paving the way for financial losses to occur: • Breach leading to fraud • Extortion though use of personal data Loss of income/employment due to reputational damage
☐	**Bodily harm**	Negligently, knowing, or purposefully paving the way for physical injury to occur: • Suicide or other self-harm • Personal data used to track someone's location, leads to assault Medical malpractice caused by negligence or inaccuracies
☐	**Discrimination**	Harms arising from discrimination or bias (either conscious or unconscious): Entrenched bias in automated decisions

☒	**Unwarranted intrusion**	Unwanted communications or intrusions that disturb tranquillity, interrupt activities, sap time or increase the risk of other harms occurring: • Unwanted targeted advertising • Nuisance calls or spam Unwarranted surveillance
☒	**Loss of control of personal data**	Harms from thwarted expectations, through misuse, repurposing, unwanted retention or continued use and sharing of personal data, including a lack of commitment to the accuracy of data or lack of transparency: • Injury to peace of mind and ability to manage risk • Restrictions on ability to access or review use of personal data Incompatible repurposing leading to emotional distress
☐	**Lack of autonomy; manipulation and influence**	Restriction, coercion, or manipulation of people's choices or their ability to make an informed choice: • Unwarranted nudging leading to poor decisions Restriction of choice to power and information asymmetry
☒	**Psychological harms**	Negligently, knowing, or purposefully paving the way for emotional distress or disturbance (embarrassment, anxiety, fear) to occur: • Detriment to mental health • Loss of sense of control of identity • Distressed relationships • Loss of confidence • Reputational loss/loss of standing Harassment or bullying
☒	**Chilling effects**	Reduced use of service or activities due to an actual or perceived risk of potential harm. And hence, a reduction in the benefits that may have been achieved. • Reduced activities requiring good credit rating Reduced use of beneficial products or services that require sharing of data due to perceived risk
☐	**Adverse effects on the rights and freedoms**	Negative impacts on rights and freedoms in and of themselves: • Restrictions to data privacy rights • Restrictions to freedom of assembly Chilling effects on freedom of expression

9. Individual Rights

What information is being provided to data subjects?	The MyCare.scot Privacy Notice will be available to users with a link on every page of the online service, as well as being sign-posted to during sign-up and sign in. Where data from existing sources is being used, the services that users initially interacted with will have their own privacy information, including: • ScotAccount – For details of their ScotAccount ID and verified information (full name, date of birth, full address and postcode) • NHS Lanarkshire – Use of the unique CHI number, secondary care services such as appointments and vaccinations • GP Practices – Use of the unique CHI number, details from the Emergency Care Summary (medications and allergies). **December 2025 Release** For the initial release, NHS Lanarkshire will be creating patient information leaflets that link to the MyCare.scot Privacy Notice. NHS Lanarkshire will also include postcards with details and joining instructions along with dermatology appointment letters to those that are eligible to use MyCare.scot.
Is there a way for individuals to request access to their data?	The MyCare.scot Privacy Notice details how individuals can exercise their right of access to their data. For most aspects it will involve contacting the organisation responsible for their care, for example their Health Board. MyCare.scot only stores personal data temporarily (caching) when in use, but does not store data long term. But, users will be able to request a copy of the data relating to them that MyCare.scot would display. Full details of the specific process for each source of personal data will be contained within the specific documentation for that service.

Is there a way for individuals to request a correction of inaccurate or incomplete data?	The MyCare.scot Privacy Notice details how individuals can exercise their right to have inaccurate data corrected. For most aspects it will involve contacting the organisation responsible for their care, for example their Health Board. Any changes or amendments will need to be applied to the systems that MyCare.scot sources the data from. By ensuring that any rectifications are applied to the source systems, the data shown in MyCare.scot will be the most up to date records of an individual's care.
Is there a way for individuals to object to or restrict the processing of their data? Is there a way to find and delete personal data?	The MyCare.scot Privacy Notice details how individuals can exercise their right to object, restrict processing of their personal data or request data to be erased. Each request will be considered by the relevant organisation, which is likely the one responsible for providing you care (for example, your Health Board). Any changes or restrictions will need to be applied to the support services utilised by MyCare.scot. As MyCare.scot uses existing data relating to records of care users have received, it is unlikely that the underlying data will be deleted unless there is a clear reason to do so. However, each request will be considered on its own merits.
Is there a way to transfer personal data to the individual, or to another party, in a structured, commonly used and machine-readable format?	This right, commonly referred as the right to 'data portability' does not apply in this situation due to the specific legal basis relied upon for processing personal data in MyCare.scot. Therefore, this section does not apply. However, one of the reasons for MyCare.scot is to provide better access to data to individuals and the organisations providing you care, so while this specific right does not apply, the principle of making data available where it's needed is at the centre of what MyCare.scot is designed for.
Is there a way for individuals to request that they are not subject to a decision made about them based on automated profiling?	The only elements of profiling used for MyCare.scot are to determine those who are not eligible to use MyCare.scot, such as those who are under 16 years of age within NHS Lanarkshire. At the initial launch of MyCare.scot, only those who have been invited will be able to

	access MyCare.scot, with that list of individuals growing as the service is fully rolled out. The term 'automated decision making' means a decision that is made by automated means without any human involvement, that have a legal or similarly significant effect on individuals. No automated decision making occurs as part of MyCare.scot.

10. Individual Rights

Organisation Controls

All organisations involved in the Digital Front Door programme and the delivery of the MyCare.scot online service have obligations to ensure that they have appropriate organisational and technical controls in place. However, the following details relate to NES as the DFD Delivery Partner only.

Category of control	Description of organisation control
Information Security and related policy/ies	The following policies are in place and available to NES staff: • NES Corporate Information Security Policy • NES Information Security Acceptable Use Policy • NES Information Governance Policy • NES Incident Notification Management Procedures NES falls under the scope of the Security of Network and Information Systems (NIS) Regulations 2018 as an operator of an essential healthcare service. NES adheres to the Scottish Public Sector Action Plan: Cyber Resilience Framework which aligns to the NIS Regulations, the UK GDPR, and the Data Protection Act 2018.
Staff training	NES staff are mandated to undertake IG and security training on a regular basis (all new staff and then refresher training annually).

Adverse event reporting and management	All parties must follow the NHSS Information Security and Cyber Security incident reporting and management process. Details of NES's protocols for handling security and confidentiality breaches are provided in the NES Incident Management Procedures. NES will report any data breaches to Controllers and/or other relevant organisations within 24 hours of discovery.
Physical access and authorisation controls	NES supports staff in hybrid working from home and the office. Each staff member is aware of their responsibilities for information security wherever they are working through the NES Corporate Information Governance and Data Protection policies available to all staff via the IG & Assurance Communications Hub. In addition: • All staff have completed mandatory NES information governance training. • Staff are using only NES supplied devices set up to NES security standards, or where staff are using their own devices, these have been assessed by NES Digital and additional security installed. No data is stored on devices.
Information asset management	NES has an Information Asset Register which is reviewed and updated on an annual basis. The Information Asset Owner should ensure that this product/processing activity is recorded on the Register.
Business continuity	NES has a Business Continuity Plan which is available to all staff via the NES Intranet.
Data backup	Details of data backups will be included in the relevant product-specific documentation for the services that MyCare.scot makes use of.

Technical Controls

Category of control	**Description of technical control**
System access levels and user authentication controls	MyCare.scot utilises ScotAccount functionality to control user access and the support services from the National Digital Platform to manage authentication through the use of tokens.

System auditing functionality and procedures	This aligns with Common frameworks such as ISO27001, CAF, NIST.
Encryption of special category personal data	This is done based on NHS Scotland Information Security Policy and aligns with Common frameworks such as ISO27001, CAF, NIST.
Cyber Essentials compliance	Not applicable
System Security Policy (SSP), Security Risk Assessment, and Standard Operating Procedures	These items are in place but will not be published.
Details of ISO27001/02 (if applicable)	Not applicable
Other (additional controls where applicable)	Security testing and assessment of MyCare.scot has been carried out and conforms to Scottish Public Sector Regulatory Information Security and Governance compliance standards.

11. Assessing the level of risk

The risk terminology for this DPIA is:

- **Risk:** the chance of something happening or a hazard being realised, which will have an impact on processing activities.
- **Risk Impact:** the outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
- **Risk Likelihood:** a measure of the probability that the consequence will occur, as a qualitative description of synonym.
- **Risk Score:** the 'score' that a risk is given following a risk assessment.

			Likelihood				
			Rare	Unlikely	Possible	Likely	Almost Certain
		Score	1	2	3	4	5
Impact	Catastrophic	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	Negligible	1	1	2	3	4	5

Risk Rating	**Combined Score**	**Action/Treatment**
High	15 - 25	Poses a serious threat. Requires immediate action to reduce/mitigate the risk.
Medium	9 - 12	Poses a threat and should be pro-actively managed to reduce/mitigate the risk.
Low	1 - 8	Poses a low threat and should continue to be monitored.

Any risk scoring higher than or equal to 15 exceeds NES's risk appetite and is likely to require further mitigation before it can be accepted. If no further mitigation is possible, the DPO and/or SIRO would need to provide their opinion/acceptance of the risk.

If a high risk cannot be reduced, prior consultation before data processing commences with the ICO is required under UK GDPR. Processing cannot go ahead until the ICO has been consulted.

Generic risks to be considered

<table>
<tr><td>1</td><td colspan="4">Risk Title: Lawfulness, fairness and transparency – Relevant legislation

There is a risk other relevant legislation has not been considered. For example, it may breach the Human Rights Act 1998, or the Common Law Duty of Confidentiality.</td></tr>
<tr><td colspan="2">Impact to the data subjects</td><td colspan="3">The impact to individuals could be their rights under certain legislation not being upheld, resulting in a loss of trust in health and social care services as a whole as well as MyCare.scot in particular.</td></tr>
<tr><td colspan="2">Privacy by design and by default notes</td><td colspan="3">Part of the Digital Front Door Programme is to ensure that all relevant legislation is considered and that the wider programme, including MyCare.scot, meets any required obligations. MyCare.scot is designed to provide better access for individuals to services and information relating to their care, and these services will also have had to consider these aspects. Considerations with regards to the ICO's Age Appropriate Design Code are included in Appendix A.</td></tr>
<tr><td colspan="2">Unmitigated risk score</td><td>Further mitigation controls required</td><td colspan="2">Residual risk score</td></tr>
<tr><td>Likelihood</td><td>3</td><td rowspan="3">As the Digital Front Door programme continues and expands the functionality of MyCare.scot, this aspect must continue to be monitored to ensure continued compliance with relevant legislation. An Equality Impact Assessment and Children's Rights and Wellbeing Impact Assessment are also being</td><td>Likelihood</td><td>1</td></tr>
<tr><td>Impact</td><td>4</td><td>Impact</td><td>4</td></tr>
<tr><td>Score</td><td>12</td><td>Score</td><td>4</td></tr>
</table>

2	**Risk Title: Lawfulness, fairness and transparency – Health/Clinical data** There is a risk that the processing of health/clinical data has not been checked or discussed with the Caldicott Guardian.				
Impact to the data subjects		No consultation with the Caldicott Guardian could result in data being processed in a way that does not align with the eight Caldicott Principles, which are designed to ensure individual's personal data relating to their care is used appropriately.			
Privacy by design and by default notes		The Caldicott Guardians of both NHS Lanarkshire and NES have been included in the consultation around the processing of personal data for MyCare.scot.			
Unmitigated risk score		*Further mitigation controls required*		*Residual risk score*	
Likelihood	3	The Caldicott Guardians will continue to be consulted as the functionality in MyCare.scot grows and expands in future.		Likelihood	1
Impact	4			Impact	4
Score	12			Score	4

3	**Risk Title: Purpose Limitation** There is a risk that the proposed processing may undergo function creep. For example, additional data fields may be requested by a stakeholder than originally identified.				
Impact to the data subjects		Function creep could cause personal data to be used or collected where it is not necessary to do so, potentially making the processing unlawful, and risks undermining the new MyCare.scot online service.			
Privacy by design and by default notes		Only data items that are necessary for that function will be used to provide the MyCare.scot online service. MyCare.scot does not store data long term and only requests the necessary items to display to the user. Any new functionality will be designed in coordination with the organisations who are responsible for your care (Health Boards and Local Authorities) to ensure that the data being used is necessary.			
Unmitigated risk score		*Further mitigation controls required*		*Residual risk score*	
Likelihood	2	As the scope of what MyCare.scot can do evolves and increases over time, the Digital Front Door Programme must ensure that new functionality remains in-line with its agreed objectives.		Likelihood	1
Impact	4			Impact	4
Score	8			Score	4

<table>
<tr><td>4</td><td colspan="4">Risk Title: Data Minimisation

There is a risk that NES does not have a procedure to review the data its holds or the processing it undergoes.</td></tr>
<tr><td colspan="2">Impact to the data subjects</td><td colspan="3">If more personal data and special category personal data is processed than is required, then this would not be in line with requirements under data protection legislation, breaching individuals' rights and potentially undermining trust in the care services as a whole.</td></tr>
<tr><td colspan="2">Privacy by design and by default notes</td><td colspan="3">All functionality available in MyCare.scot has been agreed with the organisations responsible for an individual's care, including the specific data items that are used for each aspect. MyCare.scot does not store data long term and only processes the specific items required to provide that function for a short period of time before deleting.</td></tr>
<tr><td colspan="2">Unmitigated risk score</td><td>Further mitigation controls required</td><td colspan="2">Residual risk score</td></tr>
<tr><td>Likelihood</td><td>3</td><td rowspan="3">The Digital Front Door Programme must continue to ensure data minimisation principles for any future enhancements to MyCare.scot.</td><td>Likelihood</td><td>1</td></tr>
<tr><td>Impact</td><td>4</td><td>Impact</td><td>4</td></tr>
<tr><td>Score</td><td>12</td><td>Score</td><td>4</td></tr>
</table>

<table>
<tr><td>5</td><td colspan="4">Risk Title: Storage Limitation - Retention

There is a risk that the data retention period has not been fully assessed or is too short or long.</td></tr>
<tr><td colspan="2">Impact to the data subjects</td><td colspan="3">If data is retained for too short a period, then there is a risk of that service not being able to be delivered (for example a user not being able to see their appointments information). If data is held for too long a period then there is a risk that individuals are not aware of the processing and unable to exercise their rights, as well as the processing no longer being lawful.</td></tr>
<tr><td colspan="2">Privacy by design and by default notes</td><td colspan="3">MyCare.scot does not store data long term and links to other systems where the data is stored. Data will be available when a user wishes to see it and the specialist systems that store the data are responsible for ensuring that appropriate retention periods are applied.</td></tr>
<tr><td colspan="2">Unmitigated risk score</td><td>Further mitigation controls required</td><td colspan="2">Residual risk score</td></tr>
<tr><td>Likelihood</td><td>4</td><td></td><td>Likelihood</td><td>1</td></tr>
</table>

Impact	4	Data retention considerations should continue be part of appropriate assessments when any changes or updates to MyCare.scot occur in future.	Impact	4
Score	16		Score	4

6	**Risk Title: Storage Limitation – Pseudonymised/Anonymised** There is a risk that personal data is not pseudonymised or anonymised when appropriate.

Impact to the data subjects	Pseudonymisation of data is the process of removing data items which obviously identify individuals and keep it separate from the main dataset, usually by replacing it with some form of key. A very basic example is removing names and replacing with 'person001', 'person002' and keeping a separate table (the key) that links the pseudonym (in this case 'person001') with the original data that identified someone (their name). It is a technique used to minimise data protection risks when people like data analysts don't need to know an individual's identity to perform their analysis. Pseudonymised data is still classed as personal data under data protection law. Anonymisation is the process where personal data is made completely anonymous and therefore does not identify an individual anymore. It is no longer classed as personal data under data protection legislation. The risks to data subjects if personal data is not pseudonymised/anonymised are very significant, as anonymised data is used for things like publications. This would increase the risk of confidential information being in the public domain, causing severe distress and loss of trust in public services.
Privacy by design and by default notes	Pseudonymisation and anonymisation are not required for the main uses of MyCare.scot. The only instances where pseudonymisation or anonymisation is used is when analysing people's use of the MyCare.scot online service. This data holds very few data items that could identify individuals (only a computer's IP address) which is removed before the data is used to conduct analysis. The processing is conducted under the terms of a contract and data is anonymised at the earliest opportunity.

Unmitigated risk score		*Further mitigation controls required*	*Residual risk score*	
Likelihood	4	The use of anonymisation practices when conducting analytics around the usage of MyCare.scot should continue to be	Likelihood	1
Impact	4		Impact	4
Score	16		Score	4

		monitored to ensure robust procedures remain.		

7	**Risk Title: Integrity, Confidentiality, Availability (Security) – inappropriate access** There is a risk that staff will be able to inappropriately access personal data through a lack of clear need to know policy.		
Impact to the data subjects	If staff are unaware of their responsibilities and obligations with regards to accessing sensitive data relating to the care of an individual, it could cause significant distress to individuals and damage their privacy rights.		
Privacy by design and by default notes	All NES staff must undertake information governance mandatory training annually which details their obligations with regards to handling personal data and all interactions with the data used in MyCare.scot are auditable. All NHS Scotland staff are also bound by the Code of Practice for Confidentiality.		
Unmitigated risk score		*Further mitigation controls required*	*Residual risk score*
Likelihood 3			Likelihood 1
Impact 4			Impact 4
Score 12			Score 4

8	**Risk Title: Integrity, Confidentiality, Availability (Security) – inappropriate sharing** There is a risk that personal data may be inappropriately shared with or transferred to third parties.
Impact to the data subjects	If personal data is inappropriately shared with third parties, then this could cause significant distress to individuals depending on who the third party is. It would also cause a lack of trust in the care service leading to poorer health and care outcomes.
Privacy by design and by default notes	The initial release of MyCare.scot is designed to give people access to their information. It does not share any personal data relating to an individual's health and care with other organisations except the tokens used to call the

		APIs to retrieve relevant data from source systems as described in earlier sections. A user's IP address is shared with the organisation providing usage analytics, but this is done under the terms of a contract that has processes in place to ensure handled appropriately and anonymised at the earliest opportunity.		
Unmitigated risk score		*Further mitigation controls required*	*Residual risk score*	
Likelihood	3	Any future functionality that may involve sharing of personal data with organisations or other individuals must be thoroughly reviewed to ensure it abides by data protection principles, including making individuals fully aware.	Likelihood	1
Impact	4		Impact	4
Score	12		Score	4

9	**Risk Title: Integrity, Confidentiality, Availability (Security) – technical measures** There is a risk of technical measures being absent, inadequate or untested that may result in vulnerabilities being exploited, data unintentionally damaged, destroyed, or becomes unavailable.			
Impact to the data subjects		There is a risk that if appropriate technical measures were not in place that information relating to an individual's care could become vulnerable, resulting in significant distress, infringing of their data protection rights and potentially further issues such as ID theft.		
Privacy by design and by default notes		The security of data used in MyCare.scot and the wider Digital Front Door Programme has been of utmost importance to ensure the new service creates a safe and secure means for users to interact with services. Full reviews of security implications have been undertaken and will continue to be taken, both on MyCare.scot and any of the services it uses, to ensure the safety of the data used.		
Unmitigated risk score		*Further mitigation controls required*	*Residual risk score*	
Likelihood	4	Security considerations should continue to be regularly monitored and a key part of planning on changes and enhancements to the functionality available in MyCare.scot.	Likelihood	1
Impact	5		Impact	5
Score	20		Score	5

10	**Risk Title: Accountability – Due diligence** There is a risk that due diligence has not been done on a processor or sub-processor.
Impact to the data subjects	If due diligence has not been undertaken on organisations involved in MyCare.scot, then there is a risk that the data involved may be vulnerable or exposed and not handled in line with data protection legislation. This could cause significant distress to individuals, erode trust in the service and potentially cause harm to individuals.
Privacy by design and by default notes	All Processors or sub-processors involved in MyCare.scot have had the appropriate due diligence to ensure relevant organisational and technical measures are in place.

Unmitigated risk score		*Further mitigation controls required*	*Residual risk score*	
Likelihood	4	Continue to review any processors or sub-processors at relevant intervals and ensure appropriate due diligence is conducted for any new organisations in future.	Likelihood	1
Impact	4		Impact	4
Score	16		Score	4

11	**Risk Title: Accountability – information rights** There is a risk that NES does not have a means of recognising, communication, and responding to subject access requests, or of ensuring other information requests are handled in a way that protects personal data.
Impact to the data subjects	If an individual cannot enact their information rights under data protection law, then the data protection principles are not being upheld. This means the data is potentially being processed unlawfully and that individuals cannot gain access to personal data held, or have incorrect data amended, causing distress and potentially further harm. For example if a user's address is incorrect and there is no process for handling a request to amend the information, then appointment letters could be sent to the wrong address, exposing sensitive information about the user's care to other individuals.
Privacy by design and by default notes	All organisations involved in the Digital Front Door Programme have robust processes for recognising and handling information rights requests. Clear details of each organisation's obligations are included in the relevant agreements put in place and the process for users to enact their rights are clearly detailed in the MyCare.scot Privacy Notice.

Unmitigated risk score		*Further mitigation controls required*	*Residual risk score*	
Likelihood	5		Likelihood	1
Impact	4		Impact	4
Score	20		Score	4

12	**Risk Title: Individuals Being Able to See Personal Data Relating to Others** There is a risk that if there are not robust processes in place, an individual may inadvertently be able to see personal data relating to someone else.
Impact to the data subjects	If another individual is mistakenly able to access information about a user this could cause significant distress, breaching their privacy and confidentiality and undermine trust in MyCare.scot
Privacy by design and by default notes	This risk has been treated as one of the highest priorities of the Digital Front Door Programme when devising the MyCare.scot solution. Ensuring that a user has to verify their identity first (by using ScotAccount) means that the details passed to MyCare.scot can be relied upon and the process for CHI matching uses an exact match criteria. If the situation occurs where two people have the same name, date of birth and postcode, and one of the individuals tries to sign-up to use MyCare.scot, the sign-up process would fail and the individual would not be given access to MyCare.scot. If the CHI matching process identifies more than one CHI number, then the process regards this as a failure. The individual would need to go through the alternative methods to gain access to their information where further means of confirming their identity are used.

Unmitigated risk score		*Further mitigation controls required*	*Residual risk score*	
Likelihood	4	Continue to monitor this crucial aspect of MyCare.scot and thoroughly review any changes to the sign-up or sign-in procedures to ensure controls remain robust.	Likelihood	1
Impact	5		Impact	5
Score	20		Score	5

Appendix A: DFD Considerations for the ICO Age Appropriate Design Code

The Digital Front Door web application is not considered to be a "relevant information society service" (ISS) as determined by the ICO's Age Appropriate Design Code (also referred to as the Children's Code). In the ICO's "Introduction to the Children's code" the following example is given:

A public authority which provides an online public service that is not typically provided on a commercial basis is not a relevant ISS. This is because it is not a service 'normally provided for remuneration'.

As the Digital Front Door web application is designed to provide better access to health and social care information/services, it does not meet this definition. However, whilst conforming to the code is not mandatory, it is good practice to ensure that relevant principles are followed to ensure that children's personal data is handled appropriately.

The Digital Front Door web application will initially be released in NHS Lanarkshire in December 2025 to select residents aged 16 and over. Therefore, for the purposes of the code we are considering the use of the web app by 16 and 17 year olds.

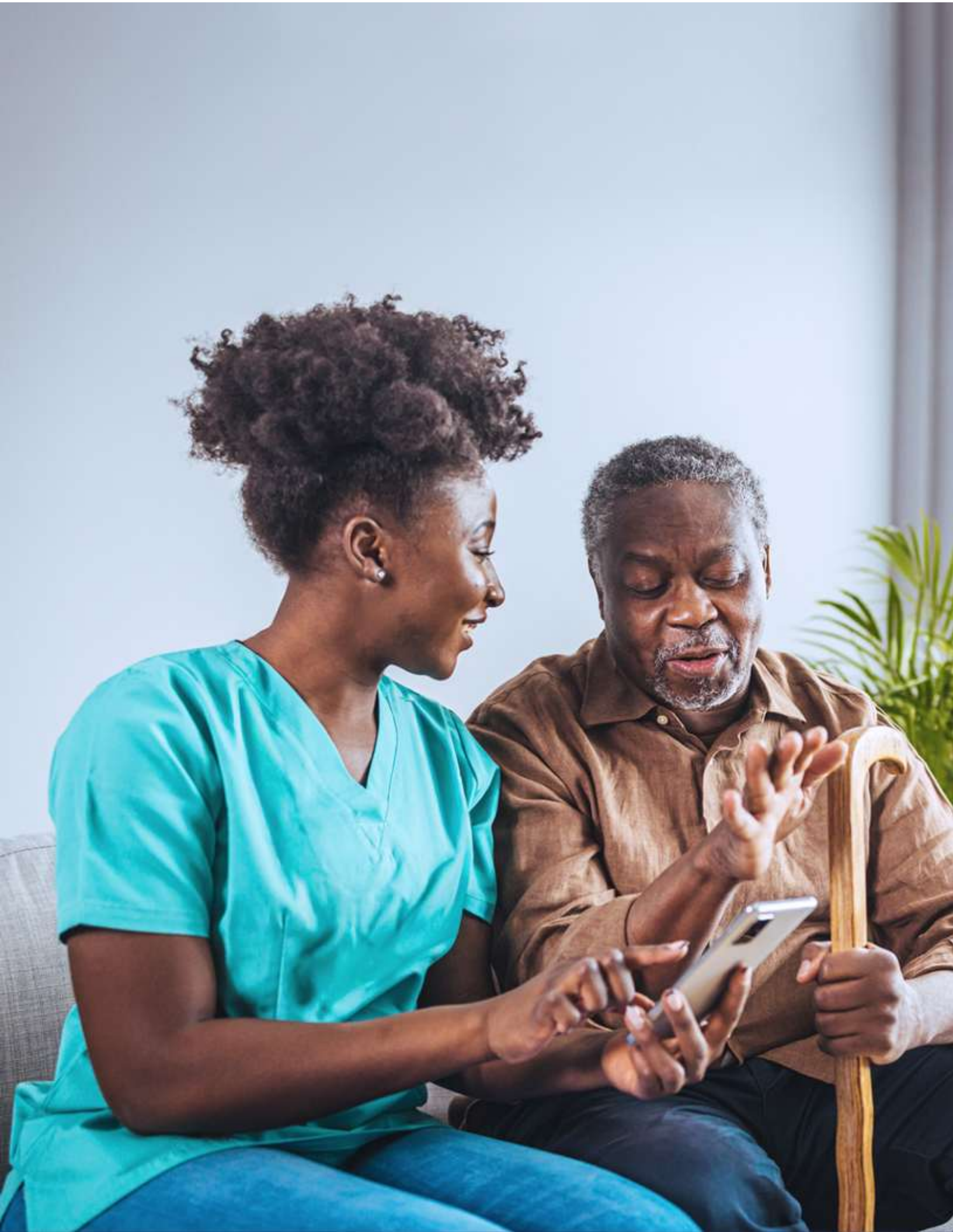
1	Best interests of the child	The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.	The purpose behind the DFD web application is to enable users to more effectively engage with health and social care services, including access to information about care they have received or are due to in future. The December 2025 release will provide the opportunity for individuals to view their demographic information, flu and covid vaccination history, allergies and prescriptions, dermatology outpatient appointment details as well as digital communications. However, for the December 2025 release, physical letters will still continue in parallel to any digital communications.
2	Data protection impact assessments	Undertake a DPIA to assess and mitigate risks to the rights and freedoms of children who are likely to access your service, which arise from your data	DPIA structure created for the work involved in DFD. This form is being used to ensure alignment with the code and will be appended to the relevant DPIAs.

		processing. Take into account differing ages, capacities and development needs and ensure that your DPIA builds in compliance with this code.	There is clinical involvement in the DFD programme to ensure that any information shown in the DFD web app is appropriate for users, including 16/17 year olds. User testing and accessibly reviews will also be undertaken.
3	Age appropriate application	Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.	Due to the fact that the DFD web app will be surfacing information about an individual's health and social care, as part of the sign-in process and matching to their unique identifying number (CHI number), it is necessary to process an individual's date of birth as part of ensuring the validity of the individual and the records being surfaced. Whilst there is no distinction between what 16/17 year-olds and the adult population will see for December 2025 release, this could be implemented for future services if required based on the data already being processed, without any further effects to the 16/17-year-olds' rights and freedoms.
4	Transparency	The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific 'bite-sized' explanations about how you use personal data at the point that use is activated.	Clear privacy information will be provided to all users of the DFD web application, with a link available on every web page of the application as well as instances where it is specifically referenced (for example initial sign-up). As per Annex B of the ICO's code, 16/17-year-olds are noted as approaching adulthood, with reasonably developed online skills, but that their technical knowledge and capabilities may be better developed than their emotional literacy. The functionality for the December 2025 release of the DFD web application will only provide the opportunity to review details of certain aspects of healthcare that have been or are planned to be provided in future, along with the new functionality of receiving digital communications, however for December 2025 release current physical letter process will continue.
5	Detrimental use of data	Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.	No personal data will be used in ways that have been shown to be detrimental to users. The DFD web app is specifically being conceived to benefit the public, including 16/17-year-olds. Clinical colleagues have been consulted on the design and use of data to ensure a user's wellbeing is one of the main considerations when creating the application.

6	Policies and community standards	Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).	All published terms and policies will be upheld, with regular reviews to ensure they continue to be up to date and match any changes to the services in future as the DFD web application grows in functionality.
7	Default settings	Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).	As the DFD web application is designed to provide users access to highly sensitive information about their health or social care, where there are different setting levels 'high privacy' will be the default for all users, including 16/17 year olds. However, for the December 2025 release, there are no relevant settings that relate to this aspect.
8	Data minimisation	Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.	The DFD web application will only use the minimum data required and does not store data long term (beyond one hour). For healthcare information this includes consulting with clinical colleagues and similar processes will be put in place for social care information when it becomes available in future. The DFD web application links to other data sources within health and social care that manages the responsibilities with regards to data retention, and the requests to share data with the DFD web application are only initiated by the user. For example, vaccinations data will only be shared with the DFD web application when the user navigates to that section within the application.
9	Data sharing	Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.	The DFD web application relies on several support systems within the public sector in order to provide the service to users. This will be clearly articulated in the privacy notice, and in most cases the sharing only occurs when the user takes actions to access information. For example, on sign-up a user must agree to share verified details from their ScotAccount to be used by the DFD web application to identify an individual's unique healthcare number (CHI Number) so that they can access the web application and their relevant information can be shown when requested. This unique identifying number is then shared with other public sector bodies who hold the relevant data the user wishes to see about their health and social care. The unique CHI number is

			transmitted by the web application to the organisation holding the data so that only the information relating to that individual is provided and then shown in the app. All instances of data sharing are necessary for the provision of the DFD web application service and are overseen by the organisation that is responsible for an individual's care (ie. a Health Board or Local Authority).
10	Geolocation	Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child). Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to 'off' at the end of each session.	There are no plans to use geolocation as part of the DFD web app.
11	Parental controls	If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.	Parental Controls will not be provided for the December 2025 release.
12	Profiling	Switch options which use profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).	There are no significant instances of profiling being used as part of the DFD web app. For December 2025 release, there will be an element of 'tactical eligibility,' where access to the app will initially be staggered to a select group of users on the first day, with more users being added at regular intervals. Those eligible will be determined by NHS Lanarkshire, the body responsible for their care, and will likely revolve around those who have newly booked dermatology appointments (which will be viewable within the app).
13	Nudge techniques	Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.	Nudge techniques are not part of the December 2025 release of the DFD web application, and will never be used to receive unnecessary personal data or weaken privacy protections.

14	Connected toys and devices	If you provide a connected toy or device ensure you include effective tools to enable conformance to this code.	The DFD web app does not support connectivity with toys and devices.
15	Online tools	Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.	The December 2025 release of the DFD web app will provide details as to how individuals (including 16/17-year-olds) can exercise their rights or report concerns. This will be through either contacting their relevant Health Board or the National Contact Centre (managed by National Services Scotland) rather than through any online tools. As the app develops and more features become available in future then available tools will be considered. However the DFD web app itself promotes transparency and better access to health and care information which individuals did not previously have, so could be considered an online tool giving them better access to their data held about them and identify any issues such as data accuracy.



Thank you