THIS IS AN NLP PRODUCED DPIA. LONDON BOROUGH OF CAMDEN'S DPO AND DATA PROTECTION MANAGER HAVE REVIEWED IT AND CONSDIER THAT IT COVERS THE RISKS AND MITIGATIONS APPROPRIATELY, AND THAT IT CAN BE ADOPTED BY LONDON BOROUGH OF CAMDEN.

DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

This DPIA template must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled or processed.

Version Control

Version	Reason	Date	Author(s)
1	New	20/05/2022	[redacted], based on SWL DPIA

Project / Work Stream Name	**Better doo Urgent Care Plan (UCP) solution**	
Project / Work Stream Lead **(Who is leading the project or implementation)**	Name	[redacted]
	Designation	CMC Strategic Commissioning
	Email	
Information Asset Owner **(Who will be responsible for the data that is stored / created)**	Name	NCL ICS SIRO?
	Designation	
	Email	
Overview: **(Summary of the project/work stream)**	Coordinate My Care (CMC) digital Urgent Care Plan is a Royal Marsden product which has been used to support consent-based care planning in preparation for future crisis or deterioration, and engagement with urgent care services within the SWL CCG footprint for the last 10 years, under contract with the CCG. This service has been expanded since 2012 to cover	

	a wider London footprint., including NCL This service has now been decommissioned with CMC ceasing in London on 31st March 2022. The new provider of the Urgent Care Plan service is Better d.o.o, a Slovenian Company. The purpose of the service is to provide a dynamic, integrated, Urgent Care Planning application for London. There is an interim arrangement for a period of approximately 3 Months where, InterSystems will continue as Processors on behalf of NCL CCG under contract. In order for the new provider to be able to provide a full service on day one (1st July 2022) there will be a data migration taking place between InterSystems and Better, this will be managed as bulk data migration 2-6 weeks prior to the service commencement date and a series of deltas between the date of the bulk and service cut-over. Better will archive, on behalf of the CCG, the data in the InterSystems data repository for patients with an active plan on 31st March 2022 and any plans created between that date and the date of cut-over so as to be able to address any data subject access requests and manage the data in accordance with the NHS Records Retention Policy. This DPIA will detail both the data migration, service cut-over and the new Urgent Care Planning service and the archiving of historic data. **Data Migration and Service Cut-Over** The migration of the service involves a number of steps as follows: The finalisation of the Better data model in openEHR that accommodates the data in the incumbent's InterSystems' bespoke data model. The finalisation and testing of the user application to display the UCP and allow users to create, edit, inactivate and archive plans. Migration of the clinical and demographic data from the current platform to the new platform as a bulk upload followed by a series of deltas, the last delta extracted at the point that the InterSystems service is put into Read Only mode before service cut-over. Transition of patients from the current solution to the new solution. The transfer of the current users from the old to the new systems and the application of suitable identity verification and authentication mechanisms. **New service information**

	The new platform is based on an openEHR data model and is designed to facilitate the rapid change to current plans and facilitate the creation and release of new care plans to users across London. A patient's UCP can be accessed (view, edit and/or create depending on user role) by identity verified and authenticated health and care professional users and supporting administrative staff in the following three contexts: a. In context with the patient's record open in an instance of either EMIS or SystmOne in general practice and other care settings that use these record systems b. In context with the patient record open in another electronic health record system such as the Cerner HIE, Cleric (London Ambulance Service Paramedics) or Adastra (NHS 111 and integrated urgent care) c. Out of context of a patient record open in another electronic health record using the Better, web based, Portal Application. The expected outcomes of adopting the Better shared care planning application (UCP) for the OneLondon Urgent Care Plan are as follows: A simple user onboarding process will result in an increased number of users and an increased number of patients with an Urgent Care Plan. A solution which will facilitate the adaption of the Urgent Care Plan to meet modern data standards for urgent care planning and the creation of new care plans for other patient groups. The application will provide role based read write access to Urgent Care Plans for all providers signed up to the use of the Urgent Care Plan provided by Better **Archiving of historic data** A data repository has been created by Better doo which will hold the historic data transferred from the InterSystems clinical data repository on behalf of the CCG as Contract Giver.
Implementation Date:	1st July 2022
Environmental Scan **Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted**	This is a replacement for an existing application.

within your organisation or by other organisations. *Please provide any supporting documents such as benefit study, fact sheets, white papers, reports or refereed articles published by industry associations, technology providers, and research centres.*	

Step 1: Complete the Screening Questions

Q	Category	Screening question	Yes/No
1.1	Technology	Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy?	No
1.2	Technology	Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data?	Yes
1.4	Identity	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	No
1.5	Multiple organisations	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
1.6	Data	Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled? *See glossary of terms*	Yes
1.7	Data	Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database?	No
1.8	Data	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	No
1.9	Data	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources?	No
1.10	Data	Will the personal data be processed out of the U.K?	Yes

Q	Category	Screening question	Yes/No
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	No
1.13	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.

Step 2: Identify the need for a DPIA									
2.1	**Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared??**							New/Changed	
								Changed	
2.2	**What data will be processed/shared/viewed?**								
	Personal Data								
	Forename	**X**	Surname	**X**	Date of Birth	**X**	Age	**X**	Gender	**X**
	Address	X	Postal address	X	Employment records		Email address	X	Postcode	X
	Other unique identifier (*please specify*)		Telephone number		Driving license number		NHS No	X	Hospital ID no	
	Other data *(Please state):*		Family / friend details for contacts; details of how to get access to premises; details of dependents/pets. Place of care preferences; organ donation preference; resuscitation preference; other wishes / cultural needs							
	Special Categories of Personal Data								
	Racial or ethnic origin		Political opinion		Religious or philosophical beliefs	*X*			
	Trade Union membership		Physical or mental health or condition		X				
	Sexual life or sexual orientation		Social service records		Child protection records				
	Sickness forms		Housing records		Tax, benefit or pension records		Adoption records		
	DNA profile		Fingerprints		Biometrics		Genetic data		
	Proceedings for any offence committed or alleged, or criminal offence record								

	Other data *(Please state):*	Any information that the person wishes to have in their care plan. This can include religious or philosophical beliefs / needs as well as requirements for treatment

Will the dataset include clinical data? (please include)	**Yes / No**
	Yes
Will the dataset include financial data?	Unlikely

Description of other data processed/shared/viewed?
Data held is decided by patient so can vary

2.3	**Business sensitive data**	**Yes/No**	**Details**
	Financial	No	**N/A**
	Local Contract conditions	No	**N/A**
	Operational data	No	**N/A**
	Notes associated with patentable inventions	No	**N/A**
	procurement/tendering information	No	**N/A**
	Customer/supplier information	No	**N/A**

Decisions impacting:	One or more business function	**Yes/No**
		No
	Across the organisation	No

Description of other data processed/shared/viewed (if any).
N/A

Step 3: Describe the sharing/processing			
3.1	**List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below*		Yes/No
			Yes
	Name	Controller or Processor?	Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
			Yes / No
	SWL CCG /ICB (from 1st July 2022)	Commissioner (they stated controller with no access to data in their DPIA, we have amended)	Yes
	GPs in NCL	Controller	Mostly
	Acute Trusts in NCL	Controller	Mostly Baseline
	London Ambulance Service	Controller	Yes
	Urgent and Emergency Care Providers in NCL	Controller	Mostly baseline
	Social Care providers in NCL	Controller	Mostly
	Better d.o.o. (UK Arm Better Ltd.)	Processor	Yes
	Care IS Ltd	Sub-processor	Yes
	Restart Ltd	Sub-processor	Yes
3.2	**If you have answered 'yes' to 3.1 is there an existing ' Data Processing Contract' or 'Data Sharing Agreement' between the Controller and the Processor?**		**Yes/No**
			Yes for Better (via SWL) Via London Care Record for rest
3.3	**Has a data flow mapping exercise been undertaken?** *If yes, please provide a copy at Annex 2 below, if no, please undertake*		Yes, see annex 1

3.4	**Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?** *If yes, provide a copy of the confidentiality agreement or contract as an annex*	Yes / No No

3.5	**Describe in as much detail why this information is being processed/shared/viewed?** *(For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use)*

Provision of Urgent care Plans. Detail of processing:

<u>Service Migration</u>

1. Data Migration
   a. Migration of the patient registry and clinical data from the incumbent supplier (InterSystems) to the new, Better, openEHR based platform of the records for all patients that have an active Urgent Care Plan defined as all those who have:
      i. Given and not withdrawn consent. It should be noted that the legal basis for the processing of the CMC plans included consent. This will apply to records that are migrated from the InterSystems solution to the new OneLondon care planning solution. Consent will not be the basis for processing of any new care plans created in the new OneLondon care planning solution.
      ii. Do not have a date of death recorded in their care plan.
      iii. Do not have a sensitive flag in the care plan.
   b. The migration plan for the clinical data is attached in the embedded document.



OneLondon Better Data Migration Spec

The key objectives of the data migration are as follows:

i. To ensure no loss of the availability of an urgent care planning solution through the transition between service providers.
ii. To map the current bespoke data model to the openEHR data model.
iii. To fully quality assure the migration of a significant data set (in excess of 10,000 records) prior to the definitive go-live migration. The quality assurance will address data loss and data fidelity, in particular for key data items such as DNACPR.
iv. To ensure the migrated data displays as expected in the new UCP Urgent Care Plan user interface and that the data provenance of key data items displays as anticipated.
v. To ensure that migrated plans can be updated and successfully saved back to the openEHR CDR.
vi. A three-stage approach will be taken
    1. Initial design verification using test or training patients recovered from the CMC data store.
    2. Quality assurance of a sample of 10,000 anonymised records. This number is required to ensure that all the clinical variation inherent in the data model is accommodated in the migration.

3. Final migration prior to go live. Following the bulk migration targeted for 2 to 6 weeks prior to go live, a series of deltas will be provided by InterSystems with the last delta being run after the InterSystems solution has been put into read only mode immediately prior to service cut-over.

2. Patient notifications: the Contract Giver and OneLondon will be responsible for the management of patient notifications.
3. User migration. The current user database will be used for the purposes of notify users of the changes that are occurring to the service and its deployment. Almost no users will be migrated to the Better authentication service because a different approach will be used to identity verification, user authentication and account creation that obviates this need. There are a limited number of use cases which may be the exception to this rule. It is currently anticipated that (some) care home users will be migrated. There may be other organisations and user groups where data will be migrated to the Better Portal authentication service. Final decisions will be made when Better has reviewed the CMC user database.
4. Service Cut-over
    a. The current supplier's application will be put into read-only mode; a final delta will be processed and imported to the Better CDR before the new UCP service is put live. During cut-over, plans will also be accessible as PDFs through the HIE.
    b. Following the close-down of the current service, data for all patients with active plans on 31st March, those who have plans created between 31st March and Service Cut-over, including those who have died between 31st March and cut-over, will be transferred by InterSystems to Better. This process will be achieved by secure file transfer. The file will be retained for Data Subject access Requests and audit. Records will be retained in accordance with the NHS Data Retention Policy and as instructed by the CCG.

New Service Information

1. The Urgent Care Plan application
    a. This is a shared care planning application. Information may be entered into the plan by health and care professionals with a legitimate relationship with the patient. The organisations that access the UCP are shown in Appendix 1. The following provides a broad categorisation of the organisations:
        i. All general practices in London
        ii. Hospices
        iii. Community Providers
        iv. Acute Trusts
        v. London Ambulance Service
        vi. Urgent and Emergency care
        vii. Care Homes (that have completed the DPST)

The London Ambulance Service users will be able to identify that a UCP exists for a patient with this NHS number and display the plan in context in the Cleric ePCR on the iPads used by the paramedics. Equally, urgent and emergency care providers that use Adastra are able to populate in real time the "Special Patient Notes" section of the patient record

A preferred method of access is through the Cerner HIE. Users authenticated by HIE are able to access either a PDF of the UCP (latest version) or to access the UCP in real time. The request header received by the Better UCP from the HIE contains user and organisation information used for audit and data

	provenance in the UCP. Mechanisms are in place to ensure that inactive plans, including plans for deceased patients, are no longer accessible through the HIE and that expired PDFs are no longer accessible. All other in context launches only identify the existence of a plan using a "General Availability Service" (GAS) and allow in-context launch. No data is passed from the Better UCP CDR to the EHR from which the plan was launched. The user views and edits the plan in an i-frame or browser.

Step 4: Assess necessity and proportionality				
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?**			
	UK GDPR	**DPA 2018**	**Other Lawful Basis**	
	Personally Identifiable Data			
	UK GDPR Article 6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…' Note that the original system erroneously used consent as the basis – this means that migrated plans may have a consent expectation. There is reasonable expectation we would migrate the plans however, but consent can be withdrawn on those.	The DPA section 8(c) – "the exercise of a function conferred on a person by an enactment or rule of law", specifically the NHS Act 2006 and the Health and Social Care Act 2012.	**N/A**	
	Special Categories of Personally Identifiable Data			
	UK GDPR Article 9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'	The DPA section 10 (1) (c) – health and social care via Schedule 1 Part 1 section 2 "Health or social care purposes" satisfying DPA section 10 (2)	N/A	
4.2	**Will the information be processed/shared electronically, on paper or both?**		Electronic	X
			Paper	X (only if patients request)
4.3	**How will you ensure data quality and data minimisation?**			
	Only data entered by patients, plus care notes where needed is held. Quality is by review by the health practitioner at creation			
4.4	**Have individuals been informed about the proposed use of their personal or special categories of personal data?** *For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to patients on their websites?*			**Yes/No** **Yes**

	Privacy notices on existing CMC system and on Better system	
4.5	**How will you help to support the rights of individuals?**	
	Existing processes; care plans are under patient control so they can edit / delete / access as they wish.	
4.6	**Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?** *If no, please describe how rights are exercised. If Yes, please detail.*	**Yes/No** **Yes**
	Existing controller arrangements; controllers will need to note if a care plan is available and include.	
4.7	**Will the processing of data include automated individual decision-making, including profiling?** *If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject*	**Yes/No** No
	N/A	
4.8	**Will individuals be asked for consent for their information to be processed/shared?** *If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.*	**Yes/No** No
	N/A – however some migrated records were consent based, so this can be a challenge.	
4.9	**As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so please complete the cloud security questionnaire and add as an annex or state below why it is not required.**	**Yes/No** Yes
	Hosted in UK Microsoft Azure which is already approved for NHS data use	
4.10	**Where will the data will be stored?** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*	
	Microsoft Azure UK West and South HSCN	
4.11	**Data Retention Period** *How long will the data be kept?*	
	In line with the NHS Records Management Code of Practice	
4.12	**Will this information being shared/processed outside the organisations listed above in question 3?** *If yes, describe who and why:*	**Yes/No** No
	N/A	

Step 5: Information Security Process							
5.1	**Is there an ability to audit access to the information?** *If no, please provide a reason why this is not required. If yes, please describe auditing.*						**Yes/No** Yes
	All access is recorded in the Better doo Audit logs. The supplier system administrators will be able to access the data. Better is ISO27001 certificated. System administrator access is managed in accordance with the ISO standard. All such access is subject to internal standard operating procedures. All access is logged, and the logs are reviewed periodically						
5.2	**How will access to information be controlled?**						
	Only health and care professionals with a legitimate relationship with the patient will have access to the UCP, where the user is able to access the same patient's record in the electronic health record system from which they are accessing the UCP (e.g. EMIS or Cleric) or explicitly controlled by admin users in each organisation or the OneLondon Urgent Care team who are employed directly by SWL CCG for the purposes of management and maintenance of the UPC						
5.3	**What roles will have access to the information?** (list individuals or staff groups)						
	Health and Care professionals with legitimate relationship to patients						
5.4	**What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?**						
	Username and password	X	Smartcard		key to locked filing cabinet/room		
	Secure 1x Token Access		Restricted access to Network Files				
	Other: *Provide a Description Below:*						
	MFA is used in many of the systems; Single-sign-on from patient record systems is leveraged for most access, but a web portal is available. Better UCP application security architecture uses industry standards including OAuth 2.0 an OpenID Connect methodologies, to cover federation, identity management and single sign-on. The solution uses RBAC as its security framework, requiring a central OpenID connect compliant SSO service for all interactions with the system. Each solution component expects a signed JWT (json web token), which is validated for each call made to the system. JWTs also contain a set of claims/roles. Each component of the solution extracts a set of permissions from the JWT, validated via RBAC. The Spring Security framework is used for token validation, role extraction and RBAC validation (see diagram at Annex 3 for flow) For information on how Better UCP application enables authenticated access to care plans from EPRs with their own local user authentication protocol, please see 'Better Platform Distributed Authentication Guide.pdf'						

5.5	**Is there a documented System Level Security Policy (SLSP) for this project? If yes, please add a copy as an annex.** SLSP is required for new systems. *SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.*		**Yes/No** Yes
	A SLSP is provided and embedded below. SLSP.pdf		
5.6	**Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?** *Please explain and give reference to such plan and protocol*		**Yes/No** Yes
	Toolkit requirement		
5.7	**Is Mandatory Staff Training in place for the following?**	**Yes/No**	**Dates**
	• Data Collection:	No	N/A – data provided by patients
	• Use of the System or Service:	Yes	Provided at take-on
	• Information Governance:	Yes	Toolkit
5.8	**Are there any new or additional reporting requirements for this project?** *If no, skip to 5.9. If yes, provide details below.*		**Yes/No** Yes
	• What roles will be able to run reports?		
	Controllers and commissioners		
	• What roles will receive the report or where will it be published?		
	Use of UCPs will be reported to boards		
	• Will the reports be in person-identifiable, pseudonymised or anonymised format?		
	Anonymised		
	• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?		

	Yes	
5.9	**Have any Information Governance risks been identified relating to this project?** If yes, the final section must be completed.	**Yes/No**

Step 6: Identify and Assess Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Falsification of UCPs by malicious persons (e.g. to provide a DNR on a person who does not want one)	High	High	High
Leakage of UCPs or access by persons without legitimate relationship	Medium	Medium	Medium
Loss of system due to resilience failures resulting in incorrect patient treatment	Medium	Medium	Medium
Providers not using UCPs due to lack of system awareness or difficult of access.	High	High	High

Step 7: Identify Measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Falsification of UCPs by malicious persons (e.g. to provide a DNR on a person who does not want one)	Verification by practitioner in presence of patient as requirement to put plan in placed	Reduced likelihood	Low	
Leakage of UCPs or access by persons without legitimate relationship	Use of authentication in EPRs as pass-through. Use of NHS single sign-on	Reduced likelihood.	Low	
Loss of system due to resilience failures resulting in incorrect patient treatment	Business continuity plans, attack resistance of HSCN	Reduced likelihood	Low	
Providers not using UCPs due to lack of system awareness or difficult of access.	Leverage existing EPRs and single-sign-on to make access easier. Provide training on UCPs to professionals as part of take-on	Reduced likelihood	Low	

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		
Residual risks approved by:		
DPO advice provided:	[redacted]	NCL GP DPO
Summary of DPO advice: All DPO advice has been incorporated into this document. Controllers are advised to ensure that appropriate training takes place to minimise risks noted.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	The DPIA will be reviewed by the respective DPOs of each organisation when required	The DPO should also review ongoing compliance with DPIA

ANNEX 1. GLOSSARY OF TERMS

Anonymised Data - means data in a form where the identity of the individual cannot be recognised i.e. when: Reference to any data item that could lead to an individual being identified has been removed; The data cannot be combined with any other data sources to produce personal identifiable data.

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 processing of personal data.

Data Flow Mapping (DFM) means the process of documenting the flows/transfers of Personal Data, Sensitive Personal Data (known as special categories personal data under UK GDPR) and Commercially Confidential Information from one location to another and the method by which they flow.

Data Subject – an individual who is the subject of personal information or can be identified from it.

Direct Care - means clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care. (National Data Guardian definition)

EPR means electronic patient record system; these are the primary systems which provide access to patient

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Special Categories of Personal Data mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

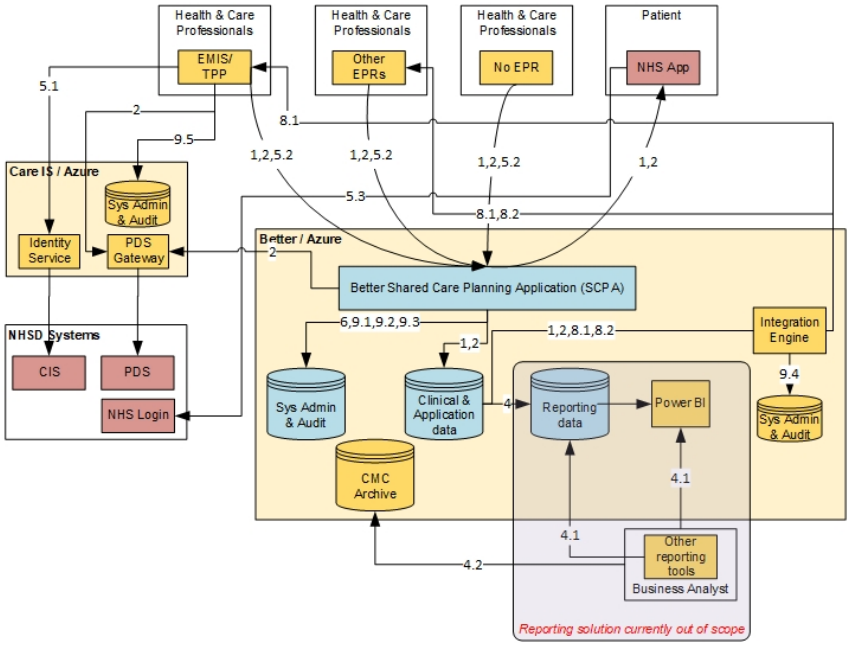
Urgent Care Plan (UCP) is a document, usually created by the patient in consultation with their healthcare professionals, detailing how they wish to be treated in a medical emergency. It can include treatments they do not wish to have and detail how and where they wish to be cared for.

For patients who have lost capacity, it is normally created in consultation with their deputies for health and welfare, or the persons they have granted with lasting power of attorney.



ANNEX 2. DATA FLOW DIAGRAM

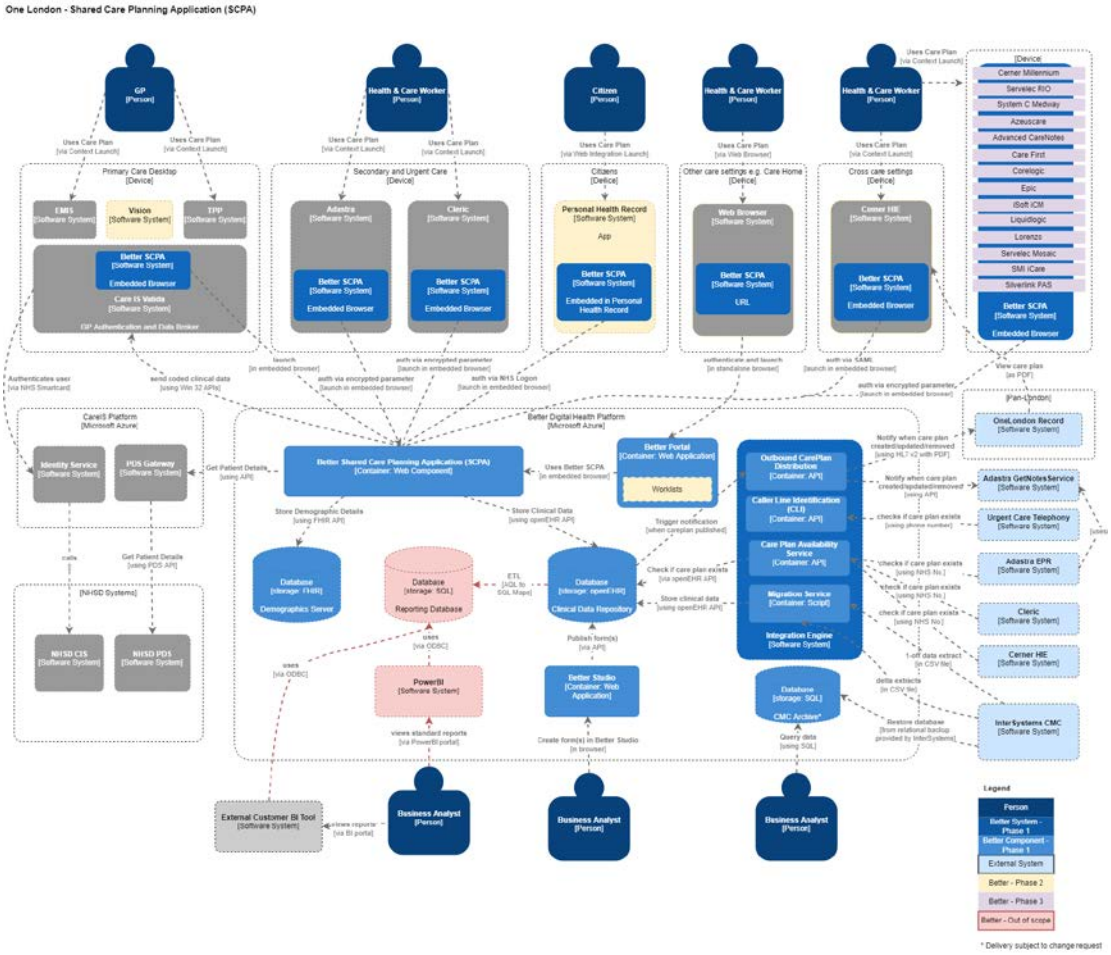
Information assets flows



Key:

1	Clinical data
2	Personal data
4.1	Reporting data
4.2	Historical reporting data
5.1	User data – Care IS Authentication Service
5.2	User data – Better Authentication Service
5.3	User data – NHS login
6	Service management data
7	HR data
8.1	Outbound interfaces – Care plan availability service
8.2	Outbound interfaces – Outbound CarePlan Distribution
9.1	Audit data – Access
9.2	Audit data – Application activity
9.3	Audit data – Data migration
9.4	Audit data – Interface activity – messaging
9.5	Audit data – Interface activity – CARE IS

System Context and Flows



ANNEX 3. UCP APPLICATION AUTHENTICATION ARCHITECTURE

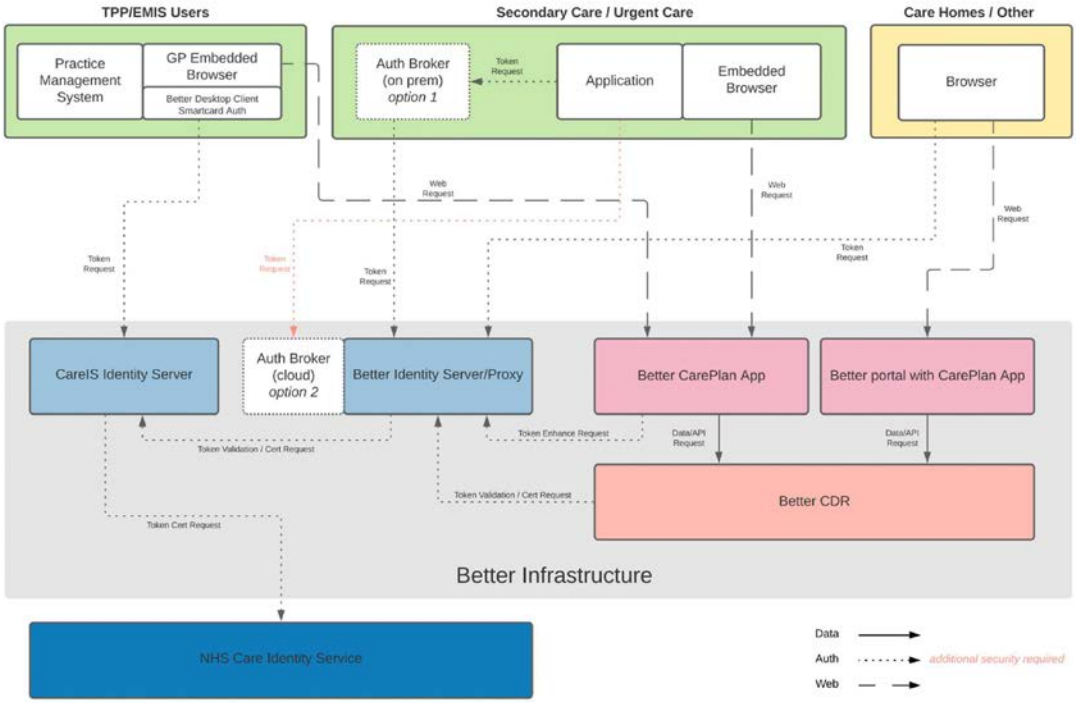


Figure 1: Better UCP application Authentication Architecture