Data Protection Impact Assessment: Child Protection Information System (CP-IS)

NHS Digital operates an IT system known as the Child Protection Information Sharing system (CP-IS). This system helps health and social care staff in England to share information about child protection plans securely, to better protect society's most vulnerable children.

When a child is known to social services and is a Looked After Child (LAC), on a Child Protection Plan (CPP) or Unborn Child Protection Plan (UCPP), basic information about that plan (referred to in this notice as CP Information) is shared securely with the NHS through CP-IS.

Throughout this document, where reference is made to a 'child on a plan' it also includes unborn children who are on a protection plan via the pregnant parent-to-be.

Within the CP-IS 'eco-system', the council and Healthcare providers are the Data Controllers for their data. NHS Digital is the Data Processor. Diagrams of the data flows can be found in Appendix A and a list of sub-processors, in Appendix B.

Background and National Consultation with Stakeholders

In 2010 The Child Health Systems Implementation Board decided that in response to Lord Laming's report a solution needed to be developed, on behalf of the Department of Health, for sharing child protection information. A working group was formed to agree the shape, scope and methodology for a new system to share child protection information. Between 2010 and 2014 the group consulted extensively with representatives from a wide range of Health Care Providers, Royal Colleges, Local Authorities and Government Departments. It had previously been acknowledged that Safeguarding extended beyond management of identified cases of abuse / neglect (child protection) to early identification for support and prevention.

Consultation asked stakeholders for their views on the types of plans that should be covered, the data items that should be shared, the types of healthcare sites that should be enabled and options analysis for benefits, technical options and governance frameworks.

The outcome was the scope as defined in the CP-IS business case (v2 2014).

As part of the consultation and scoping of CP-IS it was agreed to focus on the implementation to the following 7 NHS care settings as well as integration with Local Authority care systems:

- Emergency Departments,
- Walk-in Centres,
- Minor Injury Units,
- Ambulance services,
- GP Out of Hours & 111
- Direct access to Paediatric wards, and
- Direct access to Maternity Units

The Health and Social Care Act (2012) created the Health and Social Care Information Centre (HSCIC) with the current operational title of NHS Digital. A commencement order was created to ensure the continuity of services that had been previously instigated and/or operated from the 1st April 2014. The CP-IS was included in this process.

During the period 2014 – 2021 the service has been rolled out to over 1,200 NHS care locations within the 7 settings and to all of the 152 Local Authorities.

Stakeholders:

Government Departments and Arm's Length Bodies

Department of Health and Social Care
Department of Education
NHS England and NHS improvement
NHS England/Improvement Designated Safeguarding Leads and Networks

NHS Digital
Public Health England
National Data Guardians Office *after first draft is agreed
Information Commissioner's Office (ICO) *after first draft is agreed

Local Authorities

Association of Directors of Children's Services
Local Authority Directors of Children's Services
Children's Social Care System Suppliers

Health Care

Royal College of Emergency Medicine
Royal College of Paediatrics and Child Health
Royal College of Midwives
Royal College of Nursing
Royal College of General Practitioners
Clinical Commissioning Groups
NHS Trusts including Designated Safeguarding Nurses
Ambulance Trusts and Ambulance Safeguarding Group
Safeguarding Managers in Acute, Out of Hours, Minor Injuries, Ambulance and Walk In care settings
Community Pharmacy Leads
The Joint GP IT Committee
NHS approved and/or commissioned Information System Suppliers

The CP-IS Programme is committed to on-going stakeholder engagement to ensure the current service meets user needs. A Local Authority User Group has been set up, one of its functions being to facilitate stakeholder engagement. Representatives cover Information Governance, Business Intelligence and children's services practitioners. We have undertaken stakeholder engagement with Children and Young People, through the Office of the Children's Commissioner and Children in Care Councils.

In June and July 2021 extensive engagement was undertaken with key representatives in Local Authorities including Information Governance leads, Principal Social Workers, Caldicott Guardians and Business Intelligence leads. These sessions sought to secure support and agreement for the core service currently being delivered by CP-IS. There was unanimous support for the current service and a keen interest in supporting the development of new data sharing agreements with Local Authorities and in securing Directions.

Following these sessions, we engaged with the National Strategic Information Governance Network (SIGN) Chairs' Group, and Greater Manchester Local Authority Information Governance (GMLAIG) and Information Governance for London (IGfL) Groups.

Purpose of the processing

The purpose of the processing of data in the Child Protection - Information Sharing (CP-IS) system is to share key information regarding protected children with health and care professionals who need to know whether a child is on a protection plan or is looked after with care professionals, as they have a statutory responsibility and professional duty of care to ensure the health and wellbeing of a child.

This information is needed so health and care workers can assess the risks to the child and determine the right care and support pertaining to their health and welfare and any appropriate actions that may be necessary. This data will allow opportunity for the social worker to be informed of the attendance in any health setting and to assess whether an intervention may be necessary to safeguard and protect the child.

Sharing this data will provide care professionals with information from the CP-IS system about children subject to a Child Protection Plan (CPP), pregnant people with an Unborn Child Protection Plan (UCPP) and children who are designated a Looked After Child (LAC). These are the data subjects for CP-IS.

These are children being cared for under the following sections of the Children's Act 1989:

- Full Care Order (Section 31)
- Interim Care Order (Section 38)
- Voluntary Care Agreement (Section 20)

Health practitioners are in an opportune position to identify welfare needs or safeguarding concerns regarding individual children when they present to services and can provide support where appropriate. This includes:

- understanding risk factors,
- communicating and sharing information effectively with children and families,
- liaising with other organisations and agencies,
- assessing needs and capacity,
- responding to those needs and contributing to multi-agency assessments and reviews.

The vast majority of care settings and professionals have this safeguarding responsibility defined as part of their professional responsibilities. Health practitioners have a critical role to play in safeguarding and promoting the welfare of children including:

- GPs,
- paediatricians,
- nurses,
- health visitors,
- midwives,
- school nurses,
- allied health practitioners,
- those working in maternity,
- Great Ormond Street Hospital (unscheduled admissions & emergency transfers),
- unscheduled and emergency care settings.

Several of the above care settings have multiple tiers and focus of providing care – all of the levels are expected to be covered. The title and structure of these services can vary locally. For example, mental health has four levels of care and some specialist functions; sexual health has a broad range of services from walk in clinics through to centres for assessing sexual assault.

The scope of Phase 1 (2014 – 2020) covered:

Unscheduled care in NHS England:

- Local Authority Children's Services
- Emergency Departments
- Walk-in Centres
- Minor Injury Units
- Ambulance services
- GP Out of Hours
- Direct access to Paediatric wards
- Great Ormond Street Hospital (unscheduled admissions & emergency transfers),

Description of the Processing

CP-IS is a system with a number of different variables that can change independently. The following sections will describe those variables which can be defined as:

Who – the Health care settings that can view CP-IS

When – notification of a look-up - if event data is required to be sent to LAs

What – the type of data that flows in the system

- **Plan Data** – provided by LA's, created from the social care case management systems, and uploaded onto Spine
- **Event Data (Health alert)** – created from the RBAC profile of the person accessing the record, the organisation details and sent back to LA
- **Event Data (Audit logging)** – created from audit data held on the Spine and displayed in the CP-IS alert

How – the technical solution used to view and share data. There are three main options available to Health sites currently.

Context of the processing:

There are two prime sources of data for CP-IS – these are the 'what' of data being processed:

Record Data: This is entered by the Local Authority for any child that is in scope for CP-IS. LAs are the data controller for the plan data. This is the summary of the protection plan/looked after status for the child (as detailed in section 8 below). This includes the NHS Number (unique identifier), plan type, start date, end date and local authority contact details. This data originates from the Social Worker who inputs it directly into their Local Authority ICT product. The local ICT product automatically uploads this onto the CP-IS system (as a part of the Spine) on behalf of the Local Authority. The frequency of uploads varies according to local processes.

As the Data Processor, the only processing undertaken by NHS Digital is the application of a data quality "front door". If a data item does not meet NHS data standards, then the Local Authority record is rejected, and it is not uploaded. If the test passes, then the data is uploaded into the clinical store on the NHS Spine. The data is never altered or amended unless the LA sends an update.

The CP-IS Operations Team will contact the top ten Local Authorities with the highest number of errors to investigate and provide support to enable a new file to be uploaded. Local Authorities need to have processes in place to check and resolve their data quality issues.

Event Data: This is the summary of any presentation of a child to unscheduled care. It includes the NHS Number (unique identifier), event timestamp, organisation code and contact details for the person that accessed the record. This event data can then be used to create a Health alert for the originating LA and the NHS ICT product (or SCRa) can then automatically displays the last 25 audit records each time the screen is generated (Audit logging).

Presentation of data:

Plan Data: This is available, when a child presents for care, to NHS healthcare professionals.

Event Data for Health Care: This is available, when a child presents for unscheduled care, to NHS healthcare professionals, the last 25 such events are displayed.

Event Data for Local Authorities: This is sent back to the Local Authority as it occurs, so they have a live view on any unplanned care events. The latter is called an Access to Service Notification (ASN).

From a healthcare perspective, system access is granted by NHS England as being part of the scope of care settings that need to have sight of, and act upon, the protection status of children. As such, NHS England instructs NHS Digital to share the CP-IS data with any care settings. This provides the 'who' of data processing for sourcing and disseminating data.

The mechanism or 'how' of data dissemination is detailed below. It should be noted that the security and access control of each method are equivalent. These are best considered as simply the interface and delivery mechanism of 'what' data goes to 'who', therefore in many instances the delivery mechanisms are interchangeable where they are transporting the same clinical and administrative data.

This has been demonstrated through phase 1 of CP-IS delivery where many sites started with SCRa access to data, and since then a considerable portion have moved to integrated solutions: whereby the same data is

being shared with the same settings and sites just through a different interface mechanism with equivalent controls.

Nature and scope of the processing:

There are three existing technical solutions for health care to access CP-IS system. These are 'how' the data is transported between systems and parties. The approval for a setting to integrate with CP-IS does not dictate which integrated tool is used as sites may migrate from one method to another.

Existing technical solutions:

1. Integrated with the health care PAS system:

A care providers IT system can have CP-IS functionality built-into it. The system supplier will engage NHS Digital via the onboarding pipeline team. There is a list of functional and non-functional requirements which describe how the CP-IS functionality must operate and allows the supplier to develop against the external facing CP-IS API (Application Programming Interface). Once a supplier has developed the functionality it is assured via the NHSD accreditation processes to ensure clinical and technical compliance.

Once a system is accredited, it will automatically query the national CP-IS spine service whenever an authorised care professional conducts a PDS search. Local business processes state for this to only happen when a child is presenting in front of them. The NHS Spine will then return a near real time view of the Plan Data and Event Data. At the same time the NHS Spine will also capture audit data about the look-up (query) and use that to update the Event Data. An Access to Service Notification (ASN) is created and automatically sent to the LA that uploaded the plan.

The healthcare IT system contains a "suppression engine" to ensure that only one alert is sent to the LA and one new Event created per episode/24-hour period, per setting. The current integrated systems support unscheduled care interactions, with scheduled care interactions to be provided in a subsequent iteration.

2. Summary Care Record Application (SCRa):

The Summary Care Record Application (SCRa) is a web portal view of NHS Spine data which authorised health care professionals can access if their local IT systems do not offer CP-IS functionality. This is not to be confused with the NHSx Connecting Your Care Shared Care Record, or any other local data sharing system.

Data is pulled automatically from the national CP-IS spine service as above, as part of the existing SCRa functionality on an individual child basis. If a plan exists, the SCRa displays a tab for CP-IS (no tab is displayed if a CP-IS record does not exist). On clicking on the tab, the CP-IS record details are provided and an alert (ASN), is automatically sent back to the social care worker. The event is recorded on CP-IS as part of the unscheduled healthcare encounter history for the child. The last 25 unscheduled encounters are visible to NHS and social care staff through SCRa and their direct connect systems.

SCRa provides both Plan and Event Data. The current SCRa systems support unscheduled care interactions, with scheduled care interactions to be provided in a subsequent iteration.

Access Restrictions for Integrated solutions and SCRa

CP-IS is only visible to staff that have the appropriate Role Based Access Control (RBAC) codes added to their profile by the local organisations RA.

- B0264 – Access SCRa (Perform patient trace)
- B0107 – View Child Protection Plan

As access is person based, the tab will be visible when a member of staff is working in another setting e.g., GP authorised to view in out of hours but not in normal practice. Where a care setting is for scheduled care, they will have guidance and standard operating procedures not to activate the CP-IS tab in SCRa as that automatically creates an alert event to the social care worker as if a child had presented at unscheduled healthcare. There is an auditing function within SCRa to periodically police this.

Reporting and Monitoring

There is a requirement to provide reporting and monitoring data about the Child Protection Information Sharing (CP-IS) system. This is required both to provide the CP-IS Board with data to manage delivery/benefits and to provide Health Care and Local Authorities with a single national and regional view of safeguarding data and visibility of what data is held on the NHS Spine.

A Power BI dashboard will present the information in aggregate data in the form alongside full access control and small number suppression.

Summary Table of Care Setting, Alerts, Data and System

Each of these settings have options available to them regarding sending of alerts (to LAs) and the system used to access CP-IS.

Care Setting 'who'	**No Alert** 'when'	**Alert** 'when'	**Data** (Plan/Event)** 'what'	**System** (@@) (Integrated/SCRa/Data Extract) 'how'
Emergency Departments		Y	Plan & Event	SCRa, Integrated
Walk-in Centres		Y	Plan & Event	SCRa, Integrated
Minor Injury Units		Y	Plan & Event	SCRa, Integrated
Ambulance services		Y	Plan & Event	SCRa, Integrated
GP Out of Hours		Y	Plan & Event	SCRa, Integrated

** note that implementation to care settings may implement dissemination of Plan Data before making Event Data available.

@@ the system being used will vary across sites within a care setting. Over time there is generally a shift towards integrated solutions when suppliers have had their systems accredited.

The legal basis for the processing of personal data?

Article 6(1)c: processing is necessary for compliance with a legal obligation to which the controller is subject

Article 6(1)e: processing is necessary for the performance of a task carried out in the public interest or the exercise of the official authority vested in the controller

Processing of special categories of personal data:

Article 9(2)h: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems … with the Schedule 1, Part 2 of the DPA 2018 substantial public interest condition being paras 6 (6. Statutory and government purposes) and 18 (Safeguarding of children and individuals at risk) with the underlying law being the Children Act 2004 and the statutory guidance Working Together to Safeguard Children

Article 9(g) Reasons of substantial public interest (with a basis in law), Data Protection Act 2018 with the Schedule 1, Part 2 of the DPA 2018 substantial public interest condition being paras 6 (6. Statutory and

government purposes) and 18 (Safeguarding of children and individuals at risk) with the underlying law being the Children Act 2004 and the statutory guidance Working Together to Safeguard Children.

Fairness and proportionality

The formal safeguarding process can involve partial parental responsibility being revoked and replaced by the state to differing degrees and for differing periods. At the point that a child or unborn child is put on a child protection plan, the parents, guardians, carers and children are informed about the CP-IS system and that their child protection plan details will be shared with healthcare professionals. Local Authorities ("LA") have the responsibility of ensuring that there is a reasonable expectation that data will be used in this way in order to safeguard and promote the welfare of children.

LAs are data controllers, subject to the requirements of data protection legislation, and must provide and publish their own transparency information to explain how this data will be used. Such information will inform data subjects that healthcare settings access the child protection information and should be made accessible to the child and carers. The data that is being processed is about children, who may not be old enough to understand how data about them is used. Children still have rights to have their personal data protected and to be informed and have access to the data under the GDPR. The controllers have an obligation to ensure these rights are met and that information is made available in a manner that a child can understand.

This data is personal & special category data. It is necessary to share this data with healthcare settings to ensure that organisations can meet their obligations to the child and ensure that the child's welfare is safeguarded. The processing, whilst it may be intrusive on the privacy of the child and family, is required due to the potential of risk of harm on these vulnerable groups of children. This need overrides some of the privacy infringements, as children are now more hidden due to impact of the covid-19 pandemic and the restrictions in place in the response. It is intended that this data sharing will have a positive impact on the individuals concerned, by securing their welfare. These subjects have found themselves in a situation where their safeguarding needs override their reasonable expectation that their social care status will not be shared or their right that the data be kept private.

Consultation suggests that children are unlikely to have a more negative experience from the healthcare system as a result of this data being known, it's likely to be better and more considerate of their situation. However, some (particularly older) children may feel embarrassed about others knowing they are on a CPP or are looked after. This risk is considered to be outweighed by the benefit to the child. There may be a risk to rights and freedoms with accompanying adults, however, the system is designed to raise the issue that adults have, or may be, causing harm to the child, so there's a presumption that they would face some additional scrutiny in respect of this. In practice, this is accepted as subordinate to the (public interest) need to ensure the welfare of the child.

With regards the duty of confidence, this is overridden virtue of the statutory duty of care that these providers are subject to under the Children Act 1989, to ensure the safeguarding of children. The requirement for LAs and NHS to share information is both in statute and in professional and regulatory expectations. All local authority Children's Services departments are also expected to ensure parents and competent children they are working with are aware of privacy notices (see here, here and here for examples). This is also part of the regulatory activity on local authority children's social care undertaken by Ofsted. These informed judgements whilst may prejudice the child or family are not unwarranted, it is essential information are a required by health to ensure the right care is given and to secure the welfare of the child.

The data that is shared is kept to minimum and CP-IS information appears *ONLY IF* a child is *on/had in the past 364 days,* a protection plan, the information does *not* display if there is no CP-IS record. IF the information is displayed in an unscheduled setting, they will click on it for the summary of the plan dates and

where the plan has been created. The clicking on the information will generate an automatic notification to the social care worker that the child has presented for unscheduled care.

Although Child Protection Plans/Looked After Status close at 18 years of age, CP-IS notifies safeguarding professionals up to CPP/LAC end date + 364 days. This was a design decision that was based on the statutory and legal responsibilities around safeguarding. Professionals are required to support step-down care and local authorities still have safeguarding responsibilities for young adults. It is important to think of the two sides of CP-IS. One is the health worker viewing safeguarding data. In this case they would be viewing the fact there was a historic plan which can be considered to be part of the patient record/history. The other side is the local authority receiving an audit notification that their data was viewed. The audit contains no detail on condition or treatment. It is considered to be appropriate to support their information sharing tracking responsibilities, their responsibilities for young adults and to support step-down care.

Working Together 2018 (statutory safeguarding documentation, updated in December 2020) gives guidance on how accessing such data should be managed to ensure the rights of the individual are consider states:

- Local authorities, under section 10 of the Children Act 20045, have a responsibility to promote inter-agency co-operation to improve the welfare of all children

- Effective sharing of information between practitioners and local organisations and agencies is essential for early identification of need, assessment and service provision to keep children safe. Serious case reviews (SCRs13) have highlighted that missed opportunities to record, understand the significance of and share information in a timely manner can have severe consequences for the safety and welfare of children.

- The Data Protection Act 2018 and General Data Protection Regulations (GDPR) do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children:

    - the GDPR provides a number of bases for sharing personal information. It is not necessary to seek consent to share information for the purposes of safeguarding and promoting the welfare of a child provided that there is a lawful basis to process any personal information required. The legal bases that may be appropriate for sharing data in these circumstances could be 'legal obligation' or 'public task' which includes the performance of a task in the public interest or the exercise of official authority. Each of the lawful bases under GDPR has different requirements14. In some circumstances, it may be appropriate to obtain consent to share data but it is important to note that the GDPR sets a high standard for consent which is specific, time limited and can be withdrawn (in which case the information would have to be deleted)

- Practitioners must have due regard to the relevant data protection principles which allow them to share personal information, as provided for in the Data Protection Act 2018 and the GDPR. To share information effectively:
    - all practitioners should be confident of the lawful bases and processing conditions under the Data Protection Act 2018 and the GDPR which allow them to store and share information including information which is considered sensitive, such as health data, known under the data protection legislation as 'special category personal data'
    - where practitioners need to share special category personal data, for example, where information obtained is sensitive and needs more protection, they should always consider and identify the lawful basis for doing so under Article 6 of the GDPR, and in addition be able to meet one of the specific conditions for processing under Article 9. In effect, the Data Protection Act 2018 contains 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information, including without consent (where in the circumstances consent cannot be given, it cannot be reasonably expected that a practitioner obtains consent or if to gain consent would place a child at risk). However, practitioners should be mindful that a data protection impact assessment for any type of processing which is likely to be high risk must be completed, and therefore aware of the risks of processing special category data.

Transparency

The council's privacy notice will be amended to include this processing.

The council publishes full DPIAs

Is it necessary to collect and process all data items?

Plan Data – provided by the council, created from the social care case management systems, and uploaded onto Spine

Data Categories [*Information relating to the individual's*]	**Yes**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]*
Personal Data		
Name (Given + Family)	Yes	Required to uniquely identify the child (or parent for unborn child), in association with the NHS number
Address		N/A
Postcode		N/A
DOB	Yes	Required to uniquely identify the child (or parent for unborn child), in association with the NHS number
Age		N/A
Sex		N/A
Marital Status		N/A
Gender		N/A
Living Habits		N/A
Professional Training / Awards / Education		N/A
Income / Financial / Tax situation / Financial affairs		N/A
Email Address		N/A
Physical Description		N/A
General Identifier e.g. NHS No	Yes	Required to uniquely identify the child (or parent for unborn child), in association with the date of birth
Home Phone Number		N/A
Online Identifier e.g. IP Address/Event Logs		N/A
Website Cookies		N/A
Mobile Phone / Device No / IMEI No		N/A
Location Data (Travel / GPS / GSM Data)		N/A
Device MAC Address (Wireless Network Interface)		N/A
Banking information e.g. account number, sort code, card information		N/A
Criminal convictions / alleged offences / outcomes / proceedings / sentences		N/A
Child protection flag type	Yes	To show what type of plan a child/unborn child is on, so Health Care Workers can take the appropriate protection and health safeguarding actions. Plan types are 'Looked After Child', 'Child Protection Plan' or 'Unborn Child Protection Plan'. Entered by the Local Authority on their local system.
Plan start date	Yes	Provides context, so Health Care Workers can take the appropriate protection and health safeguarding actions. Entered by the Local Authority on their local system.
Plan end date	Yes	Provides context, so Health Care Workers can take the appropriate protection and health safeguarding actions. Entered by the Local Authority on their local system.
LA Code	Yes	Local Authority ODS code, used to identify which Local Authority the data came from and corporate parental responsibility for the child. Generated for the Local Authority on their local system.
Date time stamp	Yes	Date and time when the record was added to the Spine, used to support data processing activities.

Plan Delete Date	Yes	Not presented to Health Care Workers but is used to remove the plan from SPINE.
Local Authority Child Identity Number	Yes	LA's Unique Identifier – LA's may use a identifier other than NHS Number to uniquely identify the child. This can be included in the upload but is not surfaced to Health Care Workers.
Source Organisation Name	Yes	Name of the Local Authority
Source Organisation Emergency Duty Telephone Number	Yes	Contact Number at the Local Authority of the Emergency Duty Team.
Source Organisation Office Hours Telephone Number	Yes	Contact Number at the Local Authority
Special Category Data		
Physical / Mental Health or Condition		
Sex Life / Sexual Orientation		
Religion or Other Beliefs		
Trade Union membership		
Racial / Ethnic Origin		
Biometric Data (Fingerprints / Facial Recognition)		
Genetic Data		

Event Data – created from the RBAC profile of the person accessing the record and sent back to LA

Data Categories [*Information relating to the individual's*]	**Yes**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]*
Personal Data		
Date time stamp	Yes	Date and time when the record was accessed, used to build the access audit to be shared with health and social care
Name (prefix + Given + Family)	Yes	The name of the person accessing the record, used to build the access audit to be shared with health and social care
Job Role Code	Yes	
Job Role	Yes	The Job Title of the person accessing he record, used to build the access audit to be shared with health and social care
Organisation Code	Yes	ODS Code of the organisation from which the request originated.
Organisation Name	Yes	The organisation of the person accessing the record, used to build the access audit to be shared with health and social care
NHS Number	Yes	The NHS number of the record that was accessed.
Special Category Data		
Physical / Mental Health or Condition		
Sex Life / Sexual Orientation		
Religion or Other Beliefs		
Trade Union membership		
Racial / Ethnic Origin		
Biometric Data (Fingerprints / Facial Recognition)		
Genetic Data		

Will data be matched, combined or linked with other datasets? (internally or for external customers)

The CP-IS information provided by Social Care is linked to the patient record of the child via the Personal Demographics Service (PDS) and held on the clinical store of the Spine. NHS Digital does not link it with any other datasets.

Integrated systems use the local record as the route to request and receive data from CP-IS and will retain a copy of the data they receive linked with their local clinical records. This is essential clinical practice to ensure that all clinically relevant information is kept together as part of their contemporaneous records. They are obliged to keep this information as relevant information to support any clinical decision making or action they take. However, each time the patient record is accessed a new CP-IS search will take place to ensure the information being displayed is not out of date.

SCRa access displays the information in Spine, it does not integrate with the systems of the care professionals accessing SCRa.

Care professionals are likely to re-key the CP-IS details in their own system due to the importance of capturing and acting upon safeguarding information. They are obliged to capture any information relevant to the assessment of a child they are treating not only for their contemporaneous records but also in case, at a later data, they need to justify their actions.

What other sharing will there be

CP-IS does not share data outside of Health and Social Care. There are currently over 1,200 live sites. The full list of live sites is available on the NHS Digital website at https://digital.nhs.uk/services/child-protection-information-sharing-project/live-service-status

The *data item* will not be shared outside these organisations by our systems, however sight of the CP-IS information may prompt contact with other organisations, and it may be manually keyed into their own systems and shared verbally.

Where a care professional needs to refer a child onto other professionals for their health and care wellbeing, it is expected that the existence of the child protection order would also be shared to ensure continuity of protection context for the child to inform health and care decision making.

The council has a Multi-Agency Safeguarding Hubs (MASH) to bring together local agencies to support children, this includes protected children as well as children with other safeguarding or social care support needs. If a child presents at new unscheduled care settings and there are wider wellbeing concerns identified, then the care professionals will refer the child and their details to such groups. These groups will all be covered through NHS and/or Section 11 safeguarding responsibilities. There is an existing MAS data sharing agreement between the council, police and other agencies.

How long will the personal data be retained?

For Integrated and SCRa access to CP-IS, clinicians are viewing the live record, this view is not retained. The CP-IS information is only shown if a child is actively on a plan and during the following 364 days after the end of their last plan.

For SFTP, clinicians or child health information services (CHIS) receive a file which is then deleted after use. For CHIS, the use does include importing the information into their local system, and onward sharing with 0-19 Services, namely School Nursing and Health Visitor services. Each will keep a record in their local systems.

If the care professional re-keys the information into their own systems they will then have a record of the child being on a plan associated with the healthcare event.

Clinicians are obliged to keep contemporaneous notes including important contextual information, such as the existence of a protection plan, to demonstrate that they considered the child's full health and care context in clinical decision making and any actions they took e.g. following up any concerns colleagues. As such, the information may be inputted manually into systems when decisions are taken or by those organisations that have received a referral.

Each healthcare organisation has its own record retention rules in line with national guidance. The national guidance for record keeping for children's records are for extended periods of time. This is because children's records may be referred to many decades afterwards. For protected children this requirement is particularly relevant due to the potential concerns that may arise.

Access to CP-IS is audited, it captures the name of the person who accessed the record, their role and the date and time. If a child is Looked After or on a Child Protection Plan, it is the staff's statutory responsibility and duty to contact social care and provide details of the reason for attendance. This has been outlined within the standard operating procedure for each pilot site, with the exception of sexual health.

Accuracy and updating

Plan Data is maintained in Local Authority systems and transferred to the national CP-IS service on the NHS spine on a daily basis. CP-IS displays a view of the record as provided by the Local Authority, (live view if using integrated/SCRa, or up to 14 days if using the SEFT deltas). The accuracy and maintenance of the data is dependent on that of the Local Authority in this method of data extract.

The NHS Digital Service Operations Team maintains a data quality function which monitors error messages, failure rates and runs detailed queries on the live data. This is followed up with the relevant Local Authorities as described above in Section 4: Description of the Processing, Plan Data.

There are standard operating procedures to makes sure that alerts are made when necessary. Where a care setting is for scheduled care, they have guidance to *not* activate the CP-IS tab in SCRa as that automatically creates an alert event to the social care worker as if a child had presented at unscheduled healthcare. This is not relevant to integrated systems as they only send one alert per unscheduled episode. There is a planned enhancement to SCRa to specifically support it's use in a wider set of scheduled care settings. There are also planned additional interfaces to support scheduled care system integration.

Organisations may choose to store the data locally, but this is not recommended by the programme as there is a risk that it could become out of date on the local system if that system is not Spine connected or receives and processes updates from the local Spine connected system e.g. PAS. Any such locally stored data should clearly timestamp the CP-IS information as plan end dates do change and systems with local copies will not be notified. This has been recorded as a risk.

Data Subject Rights

The council's policies and procedures will apply

Technical and organisational controls for information security

Access Restrictions and controls

CP-IS is only visible to staff that have the appropriate RBAC codes added to their profile by the local organisations RA.

- B0264 – Access SCRa (Perform patient trace)
- B0107 – View Child Protection Plan

As access is person based, CP-IS information will be visible when a member of staff is working in another setting e.g., GP authorised to view in out of hours but not in normal practice. Where a care setting is for scheduled care, they will have guidance and standard operating procedures not to activate the CP-IS information as that automatically creates an alert event to the social care worker as if a child had presented at unscheduled healthcare. There is an auditing function within CP-IS to periodically police this.

When a child presents for healthcare treatment, they will either open SCRa alongside their existing clinical apps to record details of the encounter or if using the integrated system, it will automatically appear within their clinical application. In unscheduled care they will only look up a child that presents to them. They will access SCRa for every child that presents. This ensures that for every child they know at the beginning of the treatment whether or not they have a plan recorded against them. In this scenario we're asking them to replace their native system PDS lookup with a PDS lookup via SCRa. This is a PDS look-up which is a standard NHS Process.

Clinicians need to establish identity before they provide care. This is why they ask your name and address every time you go to A&E. They check PDS in order to find allergies, meds and conditions. This way when they are given name/address/allergies/meds they are also presented with CP-IS info if a record is present. If not, they will continue to treat the child as normal. This is why checking every child that presents, rather than just those where there is an immediate concern is not unfair/disproportionate.

When they access CP-IS information will appear *ONLY IF* a child is *on/had in the past 364 days,* a CP-IS record, the CP-IS information does *not* display if there is no CP-IS record. If the CP-IS information is displayed in an unscheduled setting, they will click on it for the summary of the plan dates and where the plan has been created. The clicking on the CP-IS information will generate an automatic notification to the social care worker that the child has presented.

For CP-IS access there is existing access control and RBAC along with auditing for all access to clinical information in general, and specifically for the CP-IS tab and related information. CP-IS access will be given to care professionals authenticated by their formal authentication. An audit is retained within SCRa of any access to CP-IS records.

Staff are trained on the use of CP-IS prior to being granted access on their smart card. All training material has been developed in conjunction with and signed off by clinical and safeguarding leads.

All sites are supported pre and post implementation of CP-IS. Guidance for the deployment of CP-IS has been provided and forms their training material and standard operating procedure. Implementation guidance include as below:

https://digital.nhs.uk/services/child-protection-information-sharing-project/implementation-process-for-healthcare-organisations/implementing-child-protection---information-sharing-using-the-summary-care-record

Location of processing

Data will be stored and processed in the UK.

Risk Assessment

The risks

Describe source of the risk and nature of potential impact on individuals	Likelihood of harm (Remote; reasonable possibility or more likely than not)	Severity of impact (Minimal impact; some impact; or serious harm	Overall risk rating (Low; medium; or high)
Unauthorised access to the CP-IS system. Failure of a Health Care Provider (HCP) / RA Manager to follow business processes, leading to unauthorised access by a healthcare professional. Lack of awareness of SOP by an unauthorised person could lead to a failure in safeguarding referrals. Malicious access by an unauthorised person could lead to inappropriate treatment and/or a breach of privacy.	Remote	Some impact	Low
Failure of Health Care provider to follow their business processes. Missing or inaccurate information (including Micro local storage of CP-IS status persisting in CP-IS records, if not updated) could limit Clinicians/professionals knowledge at point of contact with a child/young person. Over reliance on CP-IS system sending messages to the Local Authority may lead to a delay in transfer of urgent information.	Remote	Some impact	Low
Out of date / inaccurate CP-IS data due to failure of a Local Authority to follow their business processes e.g. A HCP may act on information that pertains to a different patient to the one that is intended. If this situation is not detected, this could contribute to inappropriate treatment or delay in care. CP-IS and HCP could not recognise the patient as a vulnerable child and therefore fail to notify (Social Care Provider) SCP of attendance.	Remote	Some impact	Low
Failure or poor performance of the system (including cyber-attack) would adversely impact a HCP's ability to gain access to Data stored on the Spine. This may require the HCP to	Remote	Some impact	Low

revert to alternative means of communication or not using the system. This could lead to inappropriate treatment or a delay in care and outbound messages to SCP.			
Failure of Local Authority to follow their business processes: the ‘Access to Service Notification’ (ASN) not reviewed/acted upon, due to volume of ASNs and/or lack of detail in the content, leading to a safeguarding incident / serious case review.	Remote	Some impact	Low
Privacy intrusion: some (particularly older) children may feel embarrassed about others knowing they are on a CPP or are looked after and therefore may be reluctant to seek care or treatment or share information which may help in their treatment leading to inappropriate or a delay in their care.	Reasonable possibility	Some impact	Medium
Children not uploaded onto CP-IS by Local Authorities due to lack of NHS number, or data quality issues resulting in missed safeguarding opportunities and the LA not being informed of attendances at healthcare settings.	Reasonable possibility	Some impact	Medium
Failure of a Health Care Provider to follow local business processes by not checking CP-IS leading to inappropriate treatment or a missed safeguarding opportunity and lack of notification to the Local Authority.	Reasonable possibility	Some impact	Medium

Measures to mitigate medium or high risks

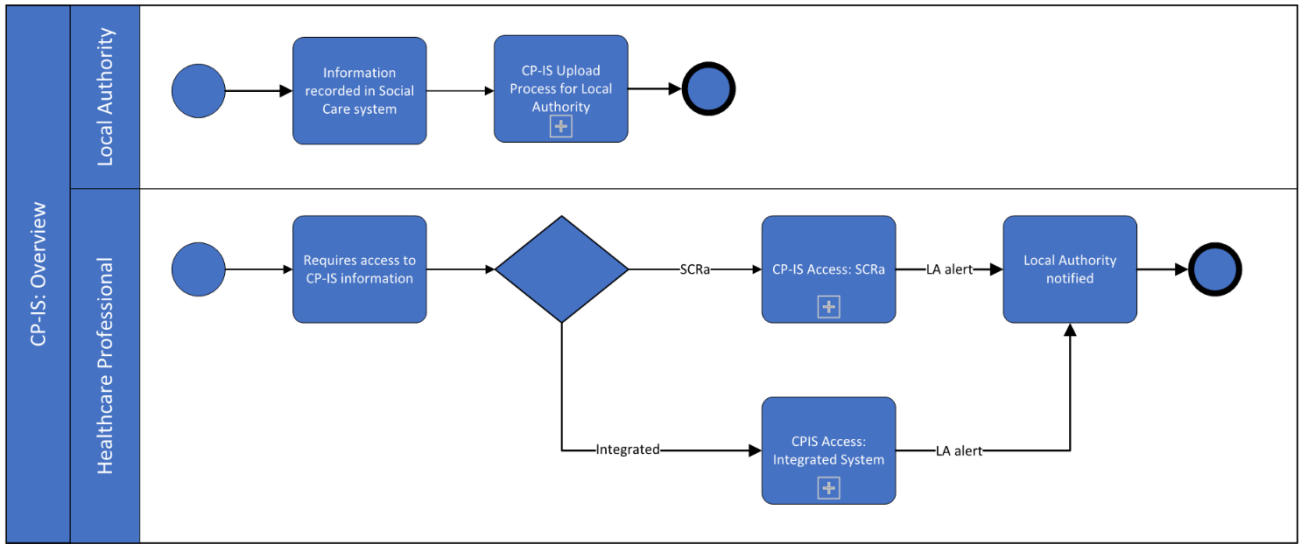
Risk	**Options to mitigate (treat) the risk**	**Effect on risk** (Tolerate / Terminate / Treat Transfer)	**Residual risk** (Low / Medium / High)	**Measure approved** (Name and Date)	**Actions integrated back into project plan** (Date and responsibility for completion)
Privacy intrusion	Minimal data processed. Risks considered proportionate to the outcomes and risks of not sharing	Tolerate	Medium	Rashida Baig 4/2/22	N/a
Data not uploaded due to data quality issues	Council has policies and procedures in place, trained staff. Lack of informing of attendance at health care settings is outwith control of council and cannot be mitigated by them	Treat	Low	Rashida Baig 4/2/22	N/a
Health care provider not following practices	outwith control of council and cannot be mitigated by them	Tolerate	Medium	Rashida Baig 4/2/22	N/a

DPO advice:
I am happy with this and consider the processing appropriate
Andrew Maughan
Data Protection Officer

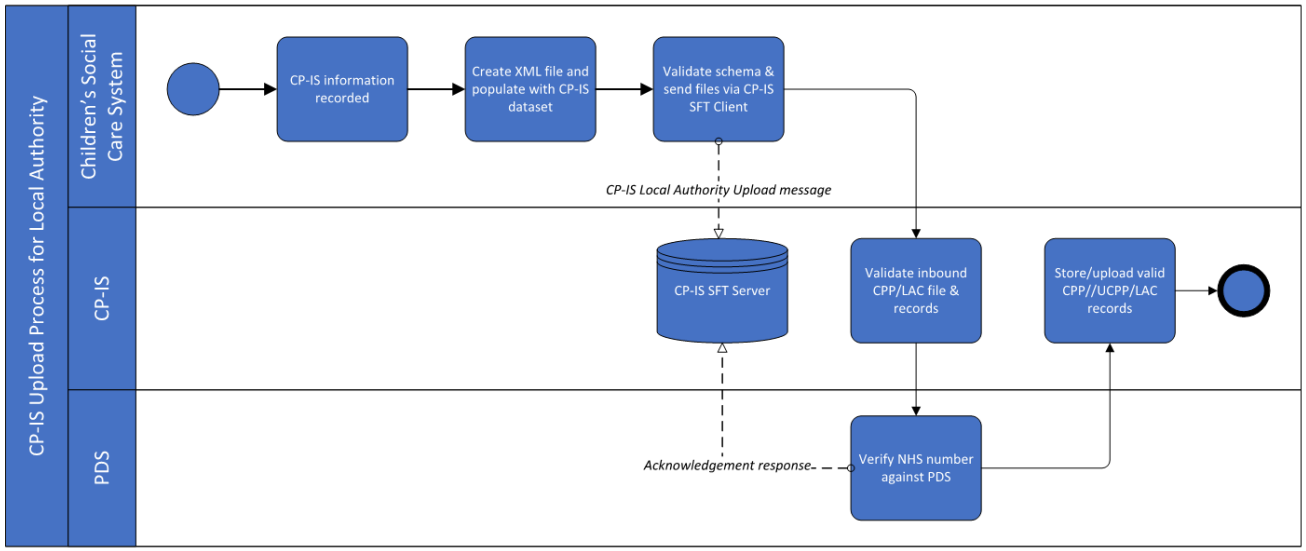
IAO Agreement: Agreed by Rashida Baig 4/2/22

Appendix A

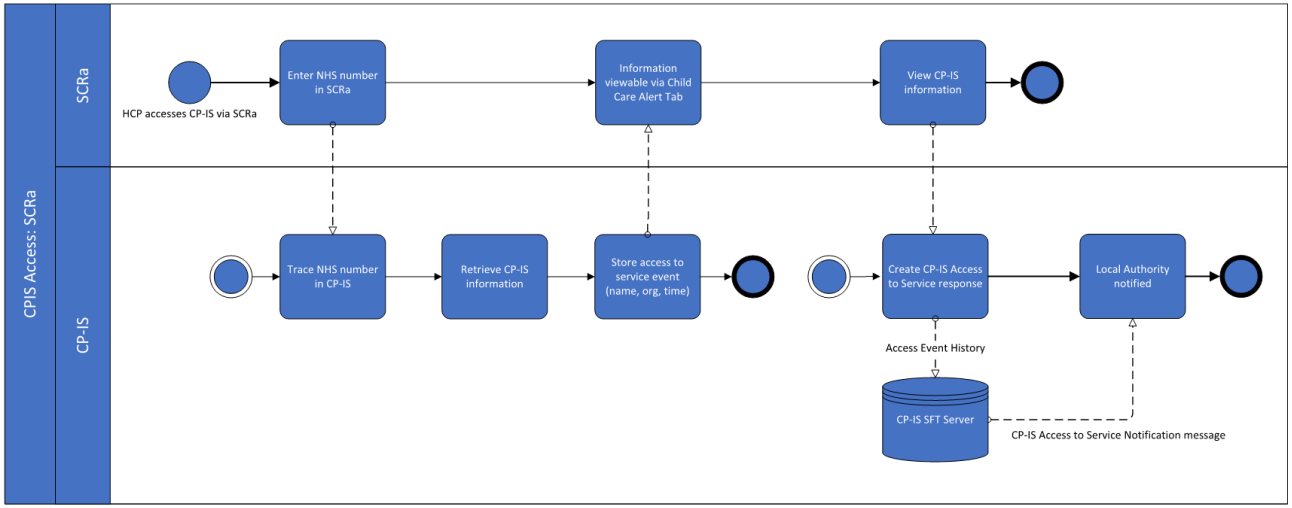
CP-IS Overview



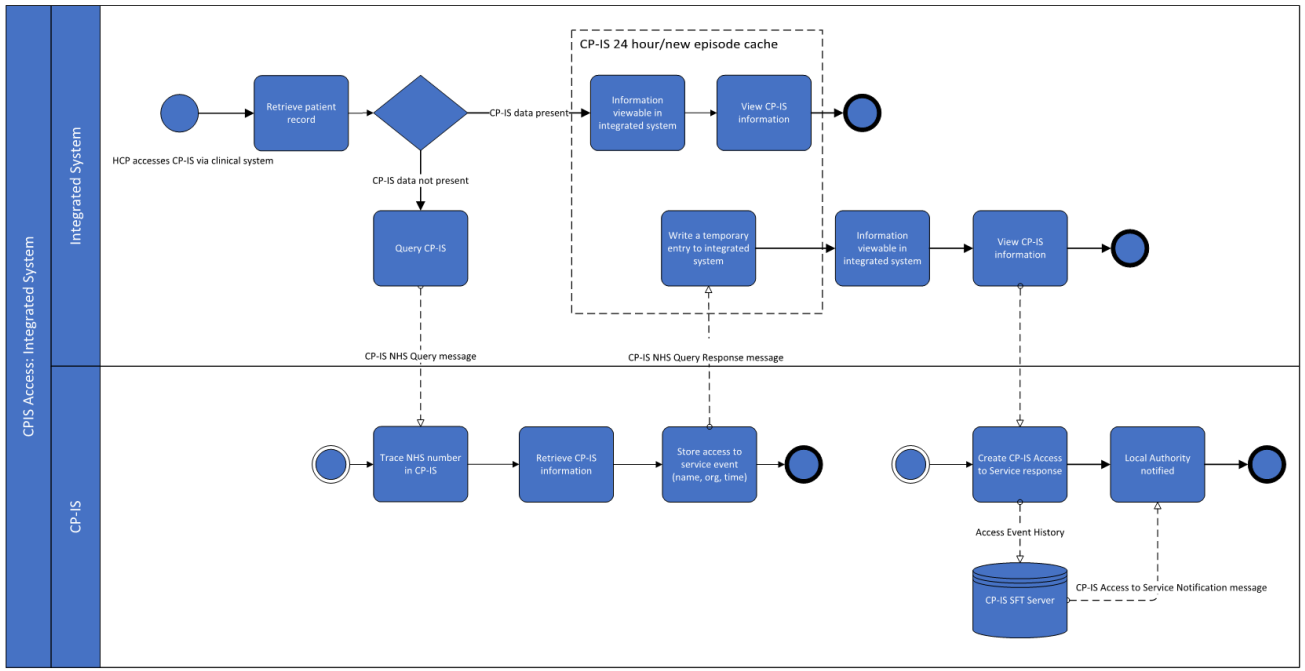
CP-IS Upload Process for Local Authority



CP-IS Access: SCRa



CP-IS Access: Integrated System


CPIS Access: Integrated System
Integrated System
CP-IS
CP-IS 24 hour/new episode cache
HCP accesses CP-IS via clinical system
Retrieve patient record
CP-IS data present
Information viewable in integrated system
View CP-IS information
CP-IS data not present
Query CP-IS
Write a temporary entry to integrated system
Information viewable in integrated system
View CP-IS information
CP-IS NHS Query message
CP-IS NHS Query Response message
Trace NHS number in CP-IS
Retrieve CP-IS information
Store access to service event (name, org, time)
Create CP-IS Access to Service response
Local Authority notified
Access Event History
CP-IS SFT Server
CP-IS Access to Service Notification message

Appendix B

Social Care Suppliers

Supplier name	Product
Azeus	AzeusCare
Capita	One-ICS
Advanced (prev CareWorks)	CareDirector
Servelec (prev Corelogic)	Frameworki - 4.9.2.2
Servelec (prev Corelogic)	Frameworki - 4.11.0.0
Servelec (prev Corelogic)	Mosaic
Servelec (prev Tribal)	EIS
In-House Solution	SSID
Liquid Logic	LCS
OLM	Swift
OLM	Carefirst
OLM	ECLIPSE Case Management

NHS Suppliers

Supplier name	Product	Settings
Advanced Health and Care	Adastra (v3.27.00)	OOH, 111
Cerner	Millenium (v2015.1.20)	ED, Mat, Paeds, MIU
Dedalus (DXC)	Lorenzo (v3)	A&E
Dedalus (DXC)	i.PM UKI (5.1)	Any
Dedalus (DXC)	PatientCentre (6.0)	Any

EMIS	Symphony (v2.29.3) Web	ED, MIU
InterSystems	Healthcare (v2.1) Trakcare	Any
Meditech UK	Meditech (v6.0)	Any
Quicksilva	orQuestra (v2.4.1	Any
Silverlink	PCS (v3.8)	TBC
Silverlink	SMH (3.11.1.0)	Any
System C	CareFlow (previously Medway)	Any
TPP	SystmOne (version MR132)	ED, MIU, WIC, OoH
EPIC	Hyperspace	
Integrated Care 24 Ltd (iC24)	CLEO	
Advanced Health and Care	Adastra (v3.27.00)	OOH, 111
Cerner	Millenium (v2015.1.20)	ED, Mat, Paeds, MIU
Dedalus (DXC)	Lorenzo (v3)	A&E
Dedalus (DXC)	i.PM UKI (5.1)	Any
Dedalus (DXC)	PatientCentre (6.0)	Any
EMIS	Symphony (v2.29.3) Web	ED, MIU
InterSystems	Healthcare (v2.1) Trakcare	Any
Meditech UK	Meditech (v6.0)	Any
Quicksilva	orQuestra (v2.4.1	Any
Silverlink	PCS (v3.8)	TBC
Silverlink	SMH (3.11.1.0)	Any
System C	CareFlow (previously Medway)	Any
TPP	SystmOne (version MR132)	ED, MIU, WIC, OoH
EPIC	Hyperspace	
Integrated Care 24 Ltd (iC24)	CLEO	
Advanced Health and Care	Adastra (v3.27.00)	OOH, 111

Cerner	Millenium (v2015.1.20)	ED, Mat, Paeds, MIU
Dedalus (DXC)	Lorenzo (v3)	A&E
Dedalus (DXC)	i.PM UKI (5.1)	Any
Dedalus (DXC)	PatientCentre (6.0)	Any
EMIS	Symphony (v2.29.3) Web	ED, MIU
InterSystems	Healthcare (v2.1) Trakcare	Any
Meditech UK	Meditech (v6.0)	Any
Quicksilva	orQuestra (v2.4.1	Any
Silverlink	PCS (v3.8)	TBC
Silverlink	SMH (3.11.1.0)	Any
System C	CareFlow (previously Medway)	Any
TPP	SystmOne (version MR132)	ED, MIU, WIC, OoH
EPIC	Hyperspace	
Integrated Care 24 Ltd (iC24)	CLEO	
Advanced Health and Care	Adastra (v3.27.00)	OOH, 111