Data Protection Impact Assessment for

The Cleft Registry and Audit NEtwork (CRANE) Database

Document control:

	Name and role	Contact details
Document Completed by	Abhishek Dixit (AD), Data Manager / Data Scientist Kate Fitzsimons (KF), CRANE Senior Research Fellow	adixit@rcseng.ac.uk kfitzsimons@rcseng.ac.uk 020 7869 6635
Data Protection Officer name	Katarzyna Wieckowska (KW)	KWieckowska@rcseng.ac.uk 0203 797 1289
Document approved by (this should not be the same person that completes the form).	David Cromwell, CEU Director	dcromwell@rcseng.ac.uk 0207 869 6608
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Data Controller: Royal College of Surgeons of England Registration Number: Z5948910	Registration Expires: 24 October 2025

Date Completed	Version	Summary of changes
30/04/2018	V01	Draft based on NABCOP
08/05/2019	V02	Draft prepared by HW
13/05/2019	V03	Draft amended by JM
06/06/2019 – 03/10/2019	V04a-c	Draft amended by HW
31/10/2019	V05	Draft amended by JM
13/01/2020	Jan2020	Draft amended by JM
01/03/2021	Mar2021	Draft updated by JM
13/04/2021	Apr2021	Draft reviewed and signed off by KW
16/09/2025	V06	Draft updated by AD and KF

Contents

Screening questions

Please complete the following checklist:

	Section	Yes or no	N/A	Comments
1.	Does your project involve any automated decision making, evaluation or scoring including profiling and predicting using information about a person? Does the outcome from your project decide who gets access to services?	No		
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		The Cleft Registry and Audit NEtwork (CRANE) Database has both Registry and Audit functions. The CRANE Database receives patient-level information for (1) registration purposes (with section 251 approval) about children with a cleft diagnosis. This includes information on the cleft diagnosis (type, timing, diagnosing hospital), timing of contact with cleft service, sex, ethnicity, NHS number, year of birth, and details about other significant medical diagnoses that might be affecting the child (syndromes). The CRANE Database system also collects: (2) audit information on health outcomes (with explicit parental consent). Outcomes include gestational age and birth weight, height and weight, dental health, facial growth, information on speech development, psychological screening and overall health; (3) CRANE also collects other types of data such as date of birth and postcodes, under consent. The registration data items collected for all children (with section 251 approval) – as well as those collected with consent – are listed in the 'CRANE Database – Data Dictionary' on the CRANE website - https://www.crane-database.org.uk/resources/crane-data-dictionary/. The Data Dictionary is reviewed annually, and the last review was in February 2024.

3.	Does the proposal involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where there is an imbalance in the relationship between the position of the individual and the controller.	Yes		The CRANE Database records data on children born with cleft. For the child's outcome data to be entered into the audit database, parents must provide explicit consent. How and why we collect this data, and how the information is handled, is described in the 'CRANE Database Information Leaflet', which is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf Consent materials including this leaflet are reviewed annually, and the last review was in November 2024. If parents do not want CRANE to collect information about the care their child receives, for their cleft lip and/or palate, they can tell us at any time. They do not have to give a reason, and it will not affect the care that their child receives. Parents can ask to stop data collection at any time point if they have previously consented for CRANE to record their child's information.
4.	Does your project involve any innovative use or applying new technological or organisational solutions? This could include biometric or genetic data, the tracking of individuals' location or behaviour?	No		
5.	Does your project match data or combine datasets from different sources?	Yes		The CRANE Database may link its consented cases to the following datasets: Hospital Episode Statistics (HES) provided by NHS England, Patient Episode Statistics for Wales provided by Wales Information Centre, Death Register provided by Office for National Statistics (ONS), Newborn Hearing Screening Programme (NHSP) provided by NHS England and the National Pupil Database provided by the Department for Education. All database linkage activities are described in the CRANE 'Database Data Linkage Leaflet' available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Data-Linkage-Leaflet_English_Nov2024_V1.pdf.

				Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.
6.	Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Yes		Please see response to Screening Question #2, on page 4 of this document, for details on personal data collected in CRANE Database. CRANE is committed to protecting patient's privacy and always uses patient data responsibly. How we do this is described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy/ The Privacy Policy is reviewed annually, and the – last review was in January 2025.
7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	No		
8.	Is this a new project? Or have the requirements for your project changed since its initiation? Are you sharing new information or linking to new datasets that were not part of the original project specification. Have you added any new audit streams to your project?	No		

Data Protection Impact Assessment

This Data Protection Impact Assessment (DPIA) template and guide is a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. This tool will help organisations which process personal data to properly consider and address the privacy risk that this entails.

DPIA can be used alongside existing project management and risk management methodologies.

Conducting a DPIA is now a legal requirement under the GDPR (General Data Protection Regulation) which will start on the 25th May 2018 and the new UK Data Protection Act. By completing a DPIA, this will help to ensure that your project is compliant with GDPR and UK data protection legislation. This document will be updated if further ICO guidance is published or there is change in legislation.

A DPIA is the basis of a "privacy by design" approach, to help meet privacy and data protection expectations of customers, employees and other stakeholders. A DPIA is intended to be prospective and proactive and should act as an early warning system by considering privacy and compliance risks in the initial design and throughout the project.

Purpose and benefits of completing a DPIA

- A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies.
- Conducting a DPIA involves working with people within the organisation, with partner organisations and with the people affected to identify and reduce privacy risks.
- The DPIA will help determine the appropriate controls needed to protect personal data i.e. technical, procedural and physical.
- The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Conducting a DPIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.
- The ICO may often ask an organisation whether they have carried out a DPIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with Data Protection legislation.

Supplementary guidance

- Data Protection Impact Assessment under GDPR guidance
- ICO's conducting privacy impact assessments code of practice
- The ICO's Anonymisation: managing data protection risk code of practice may help organisations to identify privacy risks associated with the use of anonymised personal data.
- The ICO's Data sharing code of practice may help organisations to identify privacy risks associated with sharing personal data with other organisations.
- The ICO's codes of practice on privacy notices, as well as other more specific guidance, will also help an organisation to focus DPIAs on those issues.
- The Government Data Programme has developed a Data Science Ethical Framework to help organisations understand the benefits and risks of using personal data when developing policy. The Framework can be used as part of the process to help you describe information flows and identify privacy risks and solutions.

DPIA methodology and project information.

At what stage in the project did you conduct this DPIA? E.g. planning stage, changes to the existing project, in retrospect.

The Cleft Registry and Audit NEtwork (CRANE) Database was set up by the Department of Health in 2000. Its purpose was to collect birth, demographic and epidemiological information on all children born in England, Wales and Northern Ireland with a cleft lip and/or palate.

Starting from January 1st, 2023, CRANE has started to incorporate data from the Scottish Cleft registry and audit under consent.

This DPIA was first conducted in April 2018 as part of the checks performed to ensure the CRANE Database is compliant with GDPR and UK data protection legislation. This DPIA is reviewed and updated on a yearly basis.

Describe the overall aim of the project and the data processing you carry out

The CRANE Database collects birth, demographic and cleft diagnosis information. It also collects information about cleft-related treatment and outcomes. Please see response to Screening Question #2, on page 4 of this document, for details on the data collected in the CRANE Database.

The aims of the CRANE Database are:

1. to register birth, demographic and epidemiological data related to all children born in England, Wales and Northern Ireland with the congenital abnormalities of cleft lip and/or palate.
2. to register birth, demographic and epidemiological data related to consented children born in Scotland with the congenital abnormalities of cleft lip and/or palate.
3. to record (audit) the treatment of children and adults with a cleft lip and/or palate and the outcome of such treatment.

Data collected by the CRANE Database are analysed

- For the Cleft Lip and Palate Specialised Services Quality Dashboard (SSQD) on a quarterly basis https://www.england.nhs.uk/publication/specialised-services-quality-dashboards-metrics-metadata/ and
- For Annual reports that are published on the CRANE website - https://www.crane-database.org.uk/publications/.

Periodically, Hospital Episode Statistics (HES) data may be linked to the CRANE records of all CRANE-consented cases on a 5–10-year basis, for example, to conduct case ascertainment on behalf of the commissioner.

HES, NHSP and the National Pupil Database (NPD) may be used to further examine treatment and outcomes for cleft lip and/or palate (in England alone).

DPIA Consultation

We advise you to consult with as many relevant people as possible (both internal and external stakeholders**)** while conducting this assessment, consultation is an important part of a DPIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise. Consultation can take place at any point in the DPIA process and may include the project management team, Data Protection Officer, designers, IT provider, procurement team, data processors, communications team, patients, stakeholders, corporate governance and compliance teams, researchers, analysts, statisticians and senior management.

You must consult with the Data Protection Officer regarding the impacts on privacy. Please state below that you have. If you decide against seeking the views of data subjects or their representatives e.g. this would be disproportionate or impracticable, then the justification must be made clear in the box below. In the box below name the stakeholder group, date consulted and how consulted. Please insert another box if you consulted with many different stakeholder groups.

The CRANE team has consulted with the Royal College of Surgeons' (RCS) Data Protection Officer, and staff involved in the processing of CRANE information within the Clinical Effectiveness Unit (CEU) of the RCS. Furthermore, each annual review of this DPIA is approved and signed off by the CEU Director.

Publishing your DPIA report

Publishing a DPIA report is not a legal requirement, but you should consider publishing this report (or a summary or a conclusion) and you should send it to your stakeholders. Publishing the DPIA report will improve transparency and accountability, and lets individuals know more about how your project affects them. Though there may be a need to redact/remove sensitive elements e.g. information on security measures.

State in the box below if you are going to publish your DPIA. If so, please provide hyperlink to the relevant webpage if this has been done already or insert the date you intend to publish it.

This DPIA report may be shared with key stakeholders and considered for publication on the CRANE website - https://www.crane-database.org.uk/.

Data Information Flows

Please describe how personal information is collected, stored, used and deleted. Use your data flow map and information asset register to help complete this section. Explain what personal information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information. Completing this section can help identify potential 'function creep', unforeseen or unintended uses of the data for example data sharing**.**

CRANE Data Collection

NHS Trusts submit (1) registration information (with Section 251 approval) for all live births (for England, Wales, and Northern Ireland) with a cleft and (2) audit information for consented patients (alone) to the CRANE Database (including Scotland). The Trusts submit the data using the online CRANE data collection system. Each contributing Trust can only access and download the data for their own patients.

CRANE Data Storage

The CRANE data collection system is developed and hosted by Crown Informatics Limited, which is based in Retford, Nottinghamshire. When required for analysis, patient records are downloaded from the Crown online IT system onto a secure, encrypted server used by the CEU and located at the RCS. The data are held at the RCS for analysis purposes only. The CEU secure server is protected by a firewall and Intruder-detection equipment that guards the server against unauthorized access, in addition to being logically separated from the rest of RCS IT infrastructure.

CRANE Data Use

The patient-level CRANE data are used to:

1. Ensure there is an up-to-date register of all children with cleft lip and/or palate.
2. Estimate the frequency and incidence of clefting in the population.
3. Audit and report on the quality of care for patients with clefts, to promote high standards in clinical management.
4. Be linked with other national databases for validation purposes, to enhance the patient data recorded in CRANE, to reduce the data collection burden for cleft teams, and be able to more thoroughly report on the impact of cleft care on patients' outcomes.
5. Work with and receive advice from the Craniofacial Society Great Britain & Ireland (CFSGBI) to improve the delivery of cleft care in the UK.
6. Work in partnership with Specialized Commissioning Groups (SCGs) to inform commissioning of cleft services; and
7. Support research and focused studies.

CRANE Data Linkage

The CRANE data collection system holds patient identifiable information including name, NHS number, date of birth, sex, ethnicity, and postcode. Data linkage between CRANE patient data and other databases mentioned above is carried out by sending a limited and minimum dataset of identifiable information about each patient to the organization holding the official records. Patients' NHS Number is only disclosed when linking CRANE data to NHS records.

- All database linkage activities are described in the CRANE Database 'Data Linkage Leaflet' found on the CRANE website https://www.crane-database.org.uk/. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.
- All data flows are described in the 'CRANE Data Flow Diagram' found on the 'Privacy Policy' page of the audit website https://www.crane-database.org.uk/resources/privacy-policy/ reviewed annually and the last review was in January 2025.

We may be required to complete linkage with other government organisations, in the public interest.

CRANE Data Disposal

When the System or its data has completed its purpose / has become redundant or is no longer needed, the following methods will be adopted to dispose of equipment, back-up media or other stored data: (a) Old or redundant equipment holding confidential data, including hard disks and storage media, will be disposed of by physical destruction; (b) Back-up tapes will be overwritten or destroyed; (c) Confidential data will be electronically shredded using proprietary software to ensure that the data are not recoverable.

Any CRANE data extracts that are downloaded to the CEU secure server will be destroyed according to the CEU server DPIA.

CRANE Data Anonymization
Patients have the right to opt-out of outcome data collection by the CRANE Database at any time point. In such a scenario, the consent status of the patient is amended to 'declined' on the CRANE data collection system – which then proceeds to anonymize all outcome information held in the database. No further outcome information is recorded for these patients, and no outcome information is available for analysis by CRANE, once the request to opt-out has been actioned by the cleft teams providing care to the family opting out.

Guidance was provided to cleft teams in early 2020 – to amend the patient's consent status to 'declined' if patients wish to opt out of audit data collection in response to 'National data opt-out' changes (https://digital.nhs.uk/services/national-data-opt-out). In order to complement local guidance and interpretation on how to manage opting out, see https://www.crane-database.org.uk/news/national-data-opt-outs/.

Non-patient data: CRANE Contact Database
The CRANE database holds contact information on cleft team members (system users mainly) and key stakeholders who act as the contact point for CRANE. This information includes their name, organisation and contact email address and is required for administration of the audit – keeping teams informed about key audit dates and updates, for example, data submission deadlines, publication of annual reports etc. More information on this can be found on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy/.

Transferring personal data outside the European Economic Area (EEA)

If personal data is being transferred outside of the EEA, describe how the data will be adequately protected (e.g. the recipient is in a country which is listed on the Information Commissioner's list of "approved" countries, or how the data is adequately protected).

No CRANE personal data is transferred outside the EEA as part of the database hosted by Crown Informatics Ltd. If data is communicated to the CRANE team via email (not part of Standard Operating Procedure), this data will be part of Microsoft infrastructure. The College has agreed with Microsoft that all data will be stored in Manchester. However, Microsoft is still subject to US laws and therefore a data transfer to US may occur.

Justification for collecting personal data

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. In certain circumstances it may be unlawful to process information not described in the transparency information (privacy notice/fair processing material) which informs individuals how their personal data is being used.

It may not be necessary to process certain data items to achieve the purpose. They may be irrelevant or excessive leading to risk of non-compliance with the Data Protection Act.

In the tables below list and justify personal data items needed to achieve the lawful aim of a project that requires information on individuals and their personal characteristics. Insert as many more lines that you need. Work through the table of items and decide whether you should be collecting the information, examine each data field and decide if you need it.

There are two sections in the table below, one for personal data and one for personal sensitive data items.

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name	Yes		Only available to Cleft teams within hospitals to identify the patients they are registering, and adding outcome data for (as appropriate), in the CRANE Database. **Informed consent** allows the CRANE Database to collect name and surname. Names are only visible to the CRANE project team when patients have given informed consent. Names of non-consented cases are not present in any data exports made by the CRANE project team.
NHS number	Yes		Only used by Cleft teams within hospitals to identify the patients they are registering, and adding outcome data (as appropriate), in the CRANE Database. NHS number is also necessary for linkage of consented records. CRANE has **Section 251** approval to collect patients' NHS number.
Address		N/A	
Postcode	Yes		Only available to Cleft teams within hospitals to identify the patients they are registering, and adding outcome data for (as appropriate), in the CRANE Database. **Informed consent** allows the CRANE Database to collect postcode. Postcode is necessary for risk-adjusting outcomes according to relative deprivation and it is used for linkage of consented records. Postcodes are only visible to the CRANE project team when patients have given informed consent. Postcodes of non-consented cases are not present in any data exports made by the CRANE project team.
Date of birth	Yes		Used as a key identifier for Cleft teams within hospitals to identify the patients they are registering, and adding outcome data for (as appropriate), in the CRANE Database. CRANE has **Section 251** approval to collect patients' year of birth only. **Informed consent** allows the CRANE Database to collect day/month/year of birth. Date of birth is used for linkage of consented records. Days and months of birth are only visible to the CRANE project team when patients have given informed consent. Days and months of birth of non-consented cases are not present in any data exports made by the CRANE project team.
Date of death	Yes		CRANE has **Section 251** approval to collect patients' year of death. An important variable for reporting of registrations, mortality analyses and exclusions for audit analyses.
Age	Yes		Automatically generated by the CRANE Database system (from date of birth), to ensure the collection of relevant data such as outcomes at birth, at 1 year, 5 years or 10 years, respectively.
Sex	Yes		CRANE has **Section 251** approval to collect patients' sex. Important for reporting of registrations and stratification by sex in audit analyses.

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Marital Status		N/A	
Gender		N/A	
Living Habits		N/A	
Professional Training / Awards		N/A	
Income / Financial / Tax Situation		N/A	
Email Address	Yes		**CRANE contact database** Not collected for patients. Information held for extended provider (cleft cleft) teams only for administration of the audit – keeping teams informed about key audit dates and updates e.g. for data submission deadlines, and publication of annual reports.
Physical Description		N/A	
General Identifier e.g. Hospital No	No		
Home Phone Number	No		
Online Identifier e.g. IP Address/Event Logs	No		
Website Cookies	Yes		**CRANE website** Not relevant to patient data collection. Cookies are collected on the CRANE website to improve browsing experience (e.g. saving customisation settings), enabling certain functionality (e.g. logging in) and to collect anonymous data to improve the website (e.g. device/browser usage, page visit routes)
Mobile Phone / Device No	No		
Device Mobile Phone / Device IMEI No	No		
Location Data (Travel / GPS / GSM Data)	No		
Device MAC Address (Wireless Network Interface)	No		
Sensitive Personal Data			
Physical / Mental Health or Condition	Yes		Information about children's cleft type and additional diagnoses (with Section 251 approval). This is important for reporting incidence and outcomes.

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Sexual Life / Orientation		N/A	
Family / Lifestyle / Social Circumstance		N/A	
Offences Committed / Alleged to have Committed		N/A	
Criminal Proceedings / Outcomes / Sentence		N/A	
Education / Professional Training		N/A	
Employment / Career History		N/A	
Financial Affairs		N/A	
Religion or Other Beliefs		N/A	
Trade Union membership		N/A	
Racial / Ethnic Origin	Yes		CRANE has Section 251 approval to collect patients' ethnic group. Important for reporting of registrations and audit analyses. The Database started collecting information on ethnic group from 1 April 2021. In line with the mandatory recording of ethnicity within National Clinical Databases. In response to one of the eight key actions set out in July 2020 as part of the NHS response to COVID-19. To help clinicians, provider organisations and commissioners understand and address health inequality.
Biometric Data (Fingerprints / Facial Recognition)		N/A	
Genetic Data		N/A	

Data quality standards for personal data

In the box below, describe how you will ensure that personal data is accurate and kept up to date.

The cleft teams, based at the hospitals (NHS Trusts) providing healthcare and treatment to patients born with cleft lip and/or palate, are responsible for the accurate data collection and entry of their cleft patient's data into the CRANE data collection system.

The CRANE data collection system contains various validation rules for data entry to support staff for data entry and maximise data quality. CRANE data collection system allows users to export their own data to check for errors and rectify them.

Approximately once a year, or as necessary, we run data quality exercises to check for missing data and inaccuracies. Any cases that require checking or updating are notified to trusts.

Contact information held by the CRANE project team on cleft team members (system users mainly), and key stakeholders who act as the contact point for CRANE, is stored securely and used for relevant audit communications only. These contact details are kept up to date via regular communication with the users, and targeted checks every 6 months with administrators and managers within each cleft care team.

CRANE is committed to protecting patient's privacy and always using patient data responsibly. How we do this is described on the 'Privacy Policy' page of the CRANE website https://www.crane-database.org.uk/resources/privacy-policy/.

Individual's rights

If your project uses personal data, you must complete this section.

If your project uses personal data, you must state how fairness and transparency will be achieved e.g. privacy notices on websites, posters, and leaflets. The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Any information provided to children should be in such a clear and plain language that the child / vulnerable person can easily understand.

In the box below, please define the way you have ensured that individuals are aware of the rights, if they request those rights how will they achieve them? For example, if an individual requests a copy of their information held by you, describe how you would do this. You can insert any relevant policy or process guides in the appendix at the end of this document if they are not already available on your website. This section does not refer to the personal information held about your audit staff.

Individuals' rights (where relevant)	Describe how you ensure individuals are aware of these rights	Describe how you would do this	Please copy and paste section of document that states the individual's rights
Individuals are clear about how their personal data is being used.	Privacy notice on CRANE website.	Described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy/. The Privacy Policy is reviewed annually, and the last review was in January 2025.	
	Patient information leaflet on CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf	Page 2-3

		Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	
Individuals can access information held about them	Privacy notice on CRANE website.	Described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy/. The Privacy Policy is reviewed annually, and the last review was in January 2025.	
	Patient information leaflet on CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 8
Request erasure (right to be forgotten) in certain circumstances, making clear that it does not apply to an individual's health or care record, or for public health or scientific research purposes	Privacy notice on CRANE website.	Described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy. The Privacy Policy is reviewed annually, and the last review was in January 2025.	
	Patient information leaflet on CRANE website – and opt-out information	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 6-7
Rectification of inaccurate information	Privacy notice on CRANE website.	Described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy. The Privacy Policy is reviewed annually, and the last review was in January 2025.	
	Patient information leaflet on CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf.	Page 8

		Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	
Restriction of some processing	Patient information leaflet on CRANE website – and opt-out information	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Pages 6-7
Object to processing undertaken on some legal bases	Patient information leaflet on CRANE website – and opt-out information	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 6-7
Complain to the Information Commissioner's Office.	Privacy notice on CRANE website.	Described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy/.	
Withdraw consent at any time (if processing is based on consent)	Patient information leaflet on CRANE website – and opt-out information	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the – last review was in November 2024.	Page 6-7
Data portability (if relevant)	Patient information leaflet on CRANE website – and opt-out information	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 6-7

Individual knows the identity and contact details of the data controller and the data controller's data protection officer	Privacy notice on CRANE website.	Described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy/. The Privacy Policy is reviewed annually, and the last review was in January 2025.	
In which countries the data controller is processing their personal data. For data transfers outside the EU, a description of how the data will be protected (e.g. the recipient is in an 'adequate' country / how a copy of the safeguards can be obtained.	Patient information leaflet on CRANE website. No personal data is transferred outside of the NHS England, Wales and Northern Ireland.	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 1
		All database linkage activities are described in the CRANE 'Database Data Linkage Leaflet', which is available on the CRANE website https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Data-Linkage-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 1-2
To know the legal basis under which their information is processed. Is there a clear legal basis for the processing of personal data? If so, what is the legal basis?	Privacy Policy on CRANE Website	Described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy/. The Privacy Policy is reviewed annually, and the last review was in January 2025.	
To know the purpose(s) for the processing of their information.	Privacy notice on CRANE website.	Described on the 'Privacy Policy' page of the CRANE website - https://www.crane-database.org.uk/resources/privacy-policy/. The Privacy Policy is reviewed annually, and the last review was in January 2025.	
	Patient information leaflet CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website -	Page 1-3

		https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Patient information leaflet on CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 3
The source of the data (where the data were not collected from the data subject)	Patient information leaflet on CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 3
Categories of data being processed	Patient information leaflet on CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 2
	CRANE Database Data Linkage Leaflet	All database linkage activities are described in the CRANE 'Database Data Linkage Leaflet' which is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Data-Linkage-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 2
Recipients or categories of recipients	CRANE Database Data Linkage Leaflet	All database linkage activities are described in the CRANE 'Database Data Linkage Leaflet', which is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-	Page 1-2

		Information-Data-Linkage-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	
The source of the personal data	Patient information leaflet on CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/ wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 3
To know the period for which their data will be stored (or the criteria used to determine that period)	Patient information leaflet on CRANE website	'CRANE Database Information Leaflet' is available on the CRANE website - https://www.crane-database.org.uk/wp-content/uploads/2024/11/CRANE-Database-Information-Leaflet_English_Nov2024_V1.pdf. Consent materials including this leaflet are reviewed annually, and the last review was in November 2024.	Page 7-8
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	N/A		

Privacy Risks

Types of Privacy risks

- Risks affecting individuals or other third parties, for example, misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency.
- Compliance risks e.g. breach of the GDPR
- Corporate risks (to the organisation), for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public.

Risks affecting individuals

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential that the impact of the collection, use and disclosure of any patient information is considered in regard to the individual's privacy.

In the box below insert the number of individuals likely to be affected by the project. This could be the number of unique patient records your project currently holds and how many more records you anticipate receiving each year.

Data have been collected on 25,327 children diagnosed and recorded in CRANE with cleft lip and/or palate since 2000. Approximately 1000 children diagnosed with cleft lip and/or palate annually (based on registrations since 2000).

Please complete the table below with all the potential risks to the Individuals of the information you hold on them, your corporate risks and compliance risks.

When completing the table, you need to consider if:

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information, which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate and compliance risks

In the table, list the corporate risks to your organisation which could include reputational damage, loss of public trust, financial costs and data breaches. Below these, insert any compliance risks.

Possible corporate risks include:

- Non-compliance with the Data Protection Act (DPA) or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.

- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information, which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Examples of compliance risks include:

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the GDPR.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Managing Privacy and Related risks

There are many different steps you can take to reduce a privacy risk. For example,

- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors that will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Use your project plan and a detailed explanation of information flows to identify more precisely how a general risk may occur. For example, there may be certain points in a process where accidental disclosure is more likely to happen.

The DPIA actions should be added to into your project plan and risks added to your contract review documentation.

Privacy Risks and Actions Table

Please see appendix 2 for additional guidance on completing this table

What are the potential risks to the individuals whose personal data you hold?	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely (See guidance below for definition))	**Impact** 1 -Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk** **OR** **Where risk is accepted give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Unauthorised data disclosure/illegitimate access to **de-identified** patient-level data held by the CRANE	1	3	3	**A**	Ensure access to the CRANE Database System is restricted – issued only to authorised cleft team staff, and a small number of CRANE and Crown staff. In the event of sharing data with a 3rd party (only with a legitimate basis, such as consent), ensure they provide appropriate Security Assurances, are compliant with the DPA, and sign a GDPR compliant Data Sharing Agreement (DSA).	Only the CRANE staff who are directly involved in the CRANE database project (a small number of CRANE and Crown team members) have access to the data held by CRANE, which is stored securely on an encrypted server. Only authorised members from cleft services can see CRANE data held on patients treated by their service.	N/A	KF

Receipt of unsolicited personal data	3	2	5	A	Cleft teams are regularly reminded not to include PID on any communication with CRANE. These alerts are also communicated on our website. Any Cleft team sharing PID is notified immediately to avoid recurrence. CRANE policy outlines required actions when patient identifiable data (PID) is received outside of Database.	Raising awareness that sharing PID is recognised as a data breach helps educate Cleft Teams and reduces risk of this occurring. CRANE policy outlines how to safely remove unsolicited PID to avoid the risk of further disclosure.	N/A	KF
Possible loss of confidentiality, integrity or accessibility to data due to human error.	1	3	3	A	Ensure access to the CRANE Database System is restricted – issued only to authorised cleft team staff, and a small number of CRANE and Crown staff.	Only members of the CRANE Project Team have access to the data held by CRANE, which is stored securely on an encrypted server	N/A	KF
Risk of error in process, security or confidentiality of data held within Crown Informatics.	2	3	6	A	Crown Informatics complete DSPT and this means they are audited yearly regarding their compliance, processes and policies. They also run regular vulnerability scanning with various tools and are audited externally for	These practices ensure the system is protected to the highest levels available.	N/A	KF

					annual Cyber Essential plus certification. Practices such as firewall protection, patching; encryption (e.g., all system access is SSL protected to the highest levels available), multi-factor authentication / strong passwords; limiting who can access the server are all used to reduce the risk of attack and maintain the integrity of data held on the CRANE Database.			
Corporate risks & compliance risks section	**Likelihood of this happening** 1 Very unlikely 2 Unlikely 3 Possible 4 Likely 5 Very Likely (See guidance below for definition))	**Impact** 1 -Insignificant 2-Minor 3-Moderate 4-Major 5-Catastrophic (See guidance below for definition)	**Overall risk score** (likelihood x impact = score)	**Will risk be accepted, reduced or eliminated?**	**Mitigating action to reduce or eliminate each risk** **OR** **Where risk is accepted give justification.**	**Explain how this action eliminates or reduces the risk**	**Expected completion date**	**Responsible owner**
Risks to the CEU, RCS								
Unauthorised data disclosure/illegitimate access to de-identified patient-level data held by CRANE	1	4	4	**A**	Ensure access to data is restricted to those who are authorised to do so	Only the CRANE staff who are directly involved in the CRANE database project (a small number of CRANE and Crown team members) have access to the data held by	N/A	KF

						CRANE, which is stored securely on an encrypted server. Only authorised members from cleft services can see CRANE data held on patients treated by their service.		
Receipt of unsolicited personal data	3	2	5	**A**	Cleft teams are regularly reminded not to include PID on any communication with CRANE. These alerts are also communicated on our website. Any Cleft team sharing PID is notified immediately to avoid recurrence. CRANE policy outlines required actions when patient identifiable data (PID) is received outside of Database.	Raising awareness that sharing PID is recognised as a data breach helps educate Cleft Teams and reduces risk of this occurring. CRANE policy outlines how to safely remove unsolicited PID to avoid the risk of further disclosure.	N/A	KF
Possible loss of confidentiality, integrity or accessibility to data due to human error.	1	3	3	**A**	Ensure access to the CRANE Database System is restricted – issued only to authorised cleft team staff, and a small number of CRANE and Crown staff.	Only members of the CRANE Project Team have access to the data held by CRANE, which is stored securely on an encrypted server	N/A	KF

Risk of error in process, security or confidentiality of data held within Crown Informatics.	2	4	8	A	Crown Informatics complete DSPT and this means they are audited yearly regarding their compliance, processes and policies. They also run regular vulnerability scanning with various tools and are audited externally for annual Cyber Essential plus certification. Practices such as firewall protection, patching; encryption (e.g., all system access is SSL protected to the highest levels available), multi-factor authentication / strong passwords; limiting who can access the server are all used to reduce the risk of attack and maintain the integrity of data held on the CRANE Database.	These practices ensure the system is protected to the highest levels available.	N/A	KF
Targeted malicious attack at the CRANE database (towards the database itself or through social engineering).	2	4	8	A	CRANE staff undergo regular training in advanced GDPR and cyber security. Darktrace is used to scan emails containing suspicious content to deliver proactive cyber defence.	These practices ensure the system is protected to the highest levels available.	N/A	KF

					Crown Informatics run regular vulnerability scanning with various tools and are audited externally for annual Cyber Essential plus certification. Practices such as firewall protection, patching; encryption (e.g., all system access is SSL protected to the highest levels available), multi-factor authentication / strong passwords; limiting who can access the server are all used to reduce the risk of attack and maintain the integrity of data held on the CRANE Database.			

Regularly reviewing the DPIA

DPIA should be an ongoing process and regularly reviewed during the lifecycle of the project or programme to ensure

- Risks identified are still relevant
- Actions recommended to mitigate the risks have been implemented and mitigating actions are successful

You must add to your DPIA every time you make changes to the existing projects; and ensure that you incorporate any identified risks/issues to your risk/issue register for the project.

Appendix 1 Submitting your own version of DPIA

If submitting your own version of DPIA please ensure it includes the following items. If any items are missing, please add this to your DPIA and then submit it. You must also complete the screening questions above.

	Checkbox – Please tick	Evidence – Page number and section in your DPIA
Confirmation of advice /consultation sought from Data Protection Officer whilst completing the DPIA	Done	Page 9
Name of DPO	Katarzyna Wieckowska	Page 2
Name and role of person approving completion of DPIA form. This must not be the same person that completes the form.	David Cromwell, CEU Director	Page 2
Will the DPIA be published or part of it such as the summary or conclusion (not essential but encouraged). If so, where is it published?	Project Team currently feels that the 'Privacy Policy' and 'Consent documentation provide sufficient information on all key matters.	To be added if required.
Does it include a systematic description of the proposed processing operation and its purpose?	Yes	Page 9-11
Does it include the nature, scope, context and purposes of the processing	Yes	Page 9-11
Does it include personal data, recipients and period for which the personal data will be stored are recorded	Yes	Pages 9-11
Does it include the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)	Yes	Page 10
Does the DPIA explain how each individual's rights are managed? See section on individuals rights	Yes, through Privacy Policy	
Are safeguards in place surrounding international transfer? See section on sending information outside the EEA	N/A	
Was consultation of the document carried out and with whom?	Project Team, CEU, RCS and key stakeholders	Incl. Page 9
Organisations ICO registration number	Yes	Page 2
Organisations ICO registration expiry date	Yes	Page 2
Version number of the DPIA you are submitting	As per page document control section.	Page 2
Date completed	As per page document control section.	Page 2

Appendix 2 Guidance for completing the table

<table>
<tr><td>What are the potential risks to the individuals whose personal data you hold?</td><td>See examples above</td></tr>
<tr><td>Likelihood of this happening (H, M, L)</td><td>
<table>
<tr><th>Likelihood score</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Very unlikely</td><td>May only occur in exceptional circumstances</td></tr>
<tr><td>2</td><td>Unlikely</td><td>Could occur at some time but unlikely</td></tr>
<tr><td>3</td><td>Possible</td><td>May occur at some time</td></tr>
<tr><td>4</td><td>Likely</td><td>Will probably occur / re-occur at some point</td></tr>
<tr><td>5</td><td>Very likely</td><td>Almost certain to occur / re-occur</td></tr>
</table>
</td></tr>
<tr><td>Impact (H, M, L)</td><td>
<table>
<tr><th>Impact scores</th><th>Description</th><th>Example</th></tr>
<tr><td>1</td><td>Insignificant</td><td>No financial loss disruption to day to day work manageable within existing systems, no personal data loss/ no breach of confidentiality</td></tr>
<tr><td>2</td><td>Minor</td><td>Minor (<£100k) financial loss / disruption to systems; procedures require review but manageable; limited slippage in work activity, breach of confidentiality where < 20 records affected, or risk assessed as low where data pseudonymised/files encrypted and no sensitive data</td></tr>
<tr><td>3</td><td>Moderate</td><td>Disruption to financial systems (<£250k); significant slippage in work activity or resources e.g. delay in recruiting staff; procedures and protocols require significant review, breach of confidentiality/ loss personal data where < 100 records involved and no sensitive data</td></tr>
<tr><td>4</td><td>Major</td><td>Major financial loss (£500k); large scale disruption to deliverables & project plans; business activity severely undermined, wasting considerable time / resources; poor quality report leading to loss of confidence in provider, breach of confidentiality/loss of personal sensitive data or up to 1000 records</td></tr>
<tr><td>5</td><td>Catastrophic</td><td>Huge financial loss (>£500k); significant threat to viability of the organisation in total or in part; huge disruption to business activity; almost total lack of confidence in project provider, serious breach of confidentiality/loss of personal sensitive data >1000 records involved</td></tr>
</table>
</td></tr>
</table>

Risk score (calculated field)	Please multiply the likelihood by the severity (likelihood x severity = risk score). This score will help to rank the risk, so the most severe risks are addressed first
Will risk be accepted, reduced or eliminated? (where risk is accepted give justification)	A = Accepted (must give rationale/justification) R = Reduced E = Eliminated
Mitigating action to reduce or eliminate each risk	Insert here any proposed solutions – see managing privacy and related risks section above OR If a risk has been accepted, please give justification here (The purpose of the DPIA is to reduce the risk impact to an acceptable level while still allowing a useful project to be implemented.)
Explain how this action eliminates or reduces the risk	Describe how your proposed action eliminates or reduces the possible risk. You may want to assess the costs/resource requirements (i.e. purchasing additional software to give greater control over data access and retention) and balance these against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.
Expected completion date	What is the expected completion date for your proposed action? Ensure that DPIA actions are integrated into the project plan. You should continue to use the PIA throughout the project lifecycle when appropriate. The DPIA should be referred to if the project is reviewed or expanded in the future.
Action Owner	Who is responsible for this action?