Data Protection Impact Assessment for the National Cancer Audit Collaborating Centre (NATCAN)

Document control:

	Name and role	Contact details
Document Completed by	Vikki Hart, Senior Project Manager, NATCAN	VHart@rcseng.ac.uk
Data Protection Officer name	Katarzyna Wieckowska, Data Protection Officer (DPO), RCSEng	Katarzyna Wieckowska <k.wieckowska@dpocentre.com> +44 (0) 7873 705 619
Document approved by (this should not be the same person that completes the form).	Julie Nossiter, Director of Operations, NATCAN	julienossiter@rcseng.ac.uk 0207 8696601
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z5948910	

Date Completed	Version	Summary of changes
14.12.23	1.0	
18.03.24	1.1	Reviewed by JN
22.03.24	1.2	DPO review and commentary
02.04.24	1.3	Changes incorporated
17.12.24	1.4	Local patient id and how NATCAN uses this information added
25.11.25	1.5	Updated to reflect change in classification of local patient id
29.05.26	1.6	Updated links in the document

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?		N/A	
2	Does your project involve any sensitive information or information of a highly personal nature?	Yes		The NATCAN receives de-identified extracts of routine patient-level data cancer patient data in England and Wales. All patient-identifiable information is removed by the National Cancer Registration and Analysis Service (NCRAS), NHSE and the Wales Cancer Network (WCN), Public Health Wales before the data extracts are securely transferred to the NATCAN team in the CEU, RCS. In November 2025, NATCAN was notified that NHSE reclassified local patient id from 'sensitive' to an 'Identifiable' field due to the risk of potentially containing patient identifying detail. A special condition has been applied to the NATCAN DSA with NHSE to enable continued processing as follows '*..the recipient (NATCAN) will review the contents of these fields to verify whether any patient identifying details are present and permanently erase any such details in the event any are discovered.'*
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	Yes		The NATCAN receives de-identified extracts of patient-level data which is limited to a study cohort having been diagnosed with one (or more) of the following (each being defined by specific ICD codes): Bowel, Breast Cancer, Oesophago-gastric, Ovarian Cancer, Pancreatic Cancer, Prostate, Non-Hodgkin Lymphoma and Kidney Cancer, between 01.01.2015 to the Latest Available Cancer

	individual and the controller.			Registrations
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?		N/A	
5.	Does your project match data or combine datasets from different sources?	No		All datasets
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 comment in response to question 2. Information related to the legal basis for data collected by NCRAS without needing patient consent can be found here: Collecting and keeping patient data safe - NDRS (digital.nhs.uk)
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.

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.

During the planning stages of the project.

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

Aims of the project:
The Healthcare Quality Improvement Partnership (HQIP) and NHS England require access to patient data for the purpose of The National Cancer Audit Collaborating Centre (NATCAN).

NATCAN is commissioned by HQIP on behalf of NHS England and is a part of the National Clinical Audit and Patient Outcomes Programme (NCAPOP). NATCAN has been awarded to the Royal College of Surgeons of England (RCSEng) Clinical Effectiveness Unit (CEU), a collaboration between the RCSEng and the London School of Hygiene and Tropical Medicine (LSHTM).

NATCAN will deliver six new clinical audits of care delivered by NHS Providers, the audits are as follows:
• National Audit of Primary Breast cancer (NaoPri)
• National Audit of Metastatic Breast cancer (NaoMe)
• National Ovarian Cancer Audit (NOCA)
• National Pancreatic Cancer Audit (NPaCA)
• National Non-Hodgkin Lymphoma Audit (NNHLA)
• National Kidney Cancer Audit (NKCA)
NCAPOP has not previously incorporated clinical audits in these specific disease areas.

The following established audits moved into NATCAN under a contract variation in 2023:

- The Gastro-Intestinal Cancer Audit Programme (comprising the National Bowel Cancer Audit [NBOCA] and the National Oesophago-Gastric Cancer Audit [NOGCA]) on the 01.06.23
- The National Prostate Cancer Audit (NPCA) on 01.07.23

Each individual audit broadly aims to:
1. Provide regular and timely evidence to cancer services on patterns of care in England and Wales so they can benchmark their performance and identify where there is unwarranted variation.
2. Support NHS services to identify the reasons for the variation in care in order to guide quality improvement initiatives.
3. Stimulate improvements in cancer detection, treatment and outcomes including survival.

Each Audit carried out an exercise to determine their scope in Summer 2023, collaborating closely with professional groups, data partners, patient charities and patients to ensure we ask the right questions about cancer care and treatment. The scoping documents published in November 2023 identify explicit quality improvement (QI) priorities aiming to improve cancer care and outcomes that will ultimately lead to significant patient benefits.

Subsequently, each audit submitted a Quality Improvement Plan (QIP) to HQIP/NHSE in April 2024. The QIP builds on the previous Scoping Exercise and will define ten key performance indicators, and how they map to the healthcare improvement goals, national guidelines and standards (for example, the clinical guidelines and quality standards from the National Institute for Health and Care Excellence [NICE]). These key performance indicators will be used by each audit to monitor progress towards its healthcare improvement goals and to stimulate improvements in cancer care. The QIPs were published in September 2025.

Data processing:

National Disease Registration Service / NHS England will provide the RCSEng CEU with two distinct data flows. The first will be delivered on an annual cycle and is designed around the "gold standard" national cancer registry dataset. The data request covers the following pseudonymised subsets:
• National Cancer Registry Dataset (NCRD):
• Cancer Outcomes and Services Dataset (COSD)
• National Radiotherapy Dataset (RTDS)
• Systemic Anti-Cancer Therapy Dataset (SACT)
• Cancer Waiting times Dataset (CWT)
• Hospital Episodes Statistics (HES) admitted care (IP) Dataset
• HES Outpatient Dataset • HES Accident & Emergency Dataset / HES Emergency Care Dataset
• Primary Care Prescription Dataset
• Diagnostic Imaging Dataset (DIDs)
• Cancer Patient Experience Survey (CPES) Dataset
• Somatic Molecular Testing Dataset
• Office for National Statistics (ONS) death register.

The second data flow from NDRS / NHS England to the RCSEng CEU will be delivered on a quarterly basis and is designed around the release of pseudonymised extracts of the Rapid Cancer Registration Dataset (RCRD). As in the first flow, these will be linked to those national datasets listed above that are available (including COSD, CWT, RTDS, SACT, HES datasets and ONS death register).

Nine of the audits will use a cohort design with patient selection criteria based on the date of a new cancer being diagnosed. More precisely, adult patients (aged 18 and over at diagnosis) are eligible for these audits if diagnosed with any of the specified cancers (primary breast cancer, lung, ovarian, oesophago-gastric, pancreatic, prostate, non-Hodgkin lymphoma and kidney cancer) between Jan 2015 to most recent available date as per the cancer registry. The metastatic breast cancer audit covers two types of adult patients – (i) patients with a new "de novo" diagnosis of metastatic (stage 4) breast cancer, and (ii) patients who develop metastatic breast cancer due to recurrence or disease progression.

NHS England will provide the relevant records from the above-listed datasets to RCSEng CEU. The Data will contain no direct identifying data items. The Data will be pseudonymised and individuals cannot be reidentified through linkage with other data in the possession of the recipient.

Each Audit in NATCAN will carry out an Outlier Process in keeping with the updated "Detection and Management of Outliers for National Clinical Audit" guidance in England and Wales. The Audits in NATCAN will provide Trusts identified as potential alert or alarm outliers with de-identified patient-level, minimum data for all patients included in estimating the indicator for their Trust. This will provide limited but sufficient information regarding patient (for example: month and year of birth, sex, performance status), treatment (for example: procedure date) and tumour characteristics (for example: stage, risk category). The inclusion of a local patient id will enable Trusts to recognise the patient in their own identifiable data and thereby determine potential areas where improvement in practice is required.

Local Patient ID is also utilised outside of the formal outlier process to enable the Audits to provide support to Trusts when needed with their local quality improvement activities following publication of the Audit reports. On request, the Audits will also provide deidentified patient-level, minimum data for all patients included in estimating the indicator/s of interest for their Trust.

Minimal, de-identified data will be securely transferred in an encrypted, password protected extract. Local Patient ID will solely be used for the purposes stated above and will not be used for reidentification and the analysts at RCS England (LSHTM) will not reidentify any individuals for the purposes of producing the audit reports

Once in receipt of the data the RCSEng will not transfer it to any other locations. The Data will be stored on servers at the RCSEng.

The Data will be stored on servers at the RCSEng. The Data will be accessed by authorised personnel via remote access. The Data will remain on the servers at RCSEng at all times. Remote processing will only be through a secure electronic network and organisational controls prevent personnel from downloading or copying data to local devices. Remote processing will be subject to the following being in place:
• Multifactor authentication (MFA);
• Access controls granting users the minimum level of access required;
• Secure connections (e.g., VPNs or secure protocols) to protect data during remote access;
• Device security, including up-to-date software and operating systems, antivirus software, and enabled firewalls. All remote access is undertaken within the scope of the relevant organisations' DSPT (or other security arrangements as per this Data Sharing Agreement (DSA)).

The Data will not leave or be accessed outside of England at any time. The master NATCAN dataset will only be accessed by a small number of individuals within the CEU

• Data Managers at the CEU- to create extracts for each individual audit and to perform data quality checks
• IT Colleagues- to supply support to the system
• The NATCAN Director of Operations- to ensure that internal governance processes are being followed and to manage compliance with this Data Sharing Agreement
• The CEU Director- to ensure that internal governance processes are being followed and to manage compliance with this Data Sharing Agreement.

The data managers will produce subsets of the Data that will be accessed by the teams associated with each individual audit.

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.

18.03.24: NATCAN consulted with the RCSEngData Protection Officer and the Project Teams.

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

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.

The information provided to the NATCAN project team is de-identified - we do not receive any confidential patient identifiable information.

Data from Trust/Health Board data submissions are linked to selected data items from national datasets (cancer registry data, rapid registration data, HES, PEDW, ONS, RTDS and SACT) to provide information on the diagnosis, management, and treatment of people with breast, ovarian pancreatic or kidney cancer or Non-Hodgkin Lymphoma including staging, mode of admission, comorbidities, surgical procedure or intervention details, radiotherapy and chemotherapy details, readmissions and complications.

All patient identifiable information including name, address, date of birth, address, postcode and NHS number is removed by NCRAS (England) and WCN (Wales) from the data extracts before they are securely transferred to the NATCAN project team at the CEU, RCS.

NATCAN data processing carried out by the NATCAN project teams at the CEU, RCSEng
The data flow to the NATCAN is de-identified - none of the datasets received by the NATCAN project teams contain confidential patient identifiers. There is separation of identifiers and analysis datasets in the data flow (see the NATCAN dataflow for detail).

All de-identified data extracts are stored on a password protected encrypted server at the RCSEng with restricted access to named analysts in the NATCAN project team.

The NATCAN Data flows diagram can be viewed here: NATCAN Dataflow diagram - National Cancer Audit Collaborating Centre

NATCAN contact database
NATCAN holds email addresses of key functions in extended provider teams including Clinical Lead, MDT coordinator, Audit dept. and Cancer Services representatives required for administration of the audit. This is to keep teams informed about key audit dates and updates e.g data submission deadlines, publication of annual reports etc.

Refer to NATCAN 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).

N/A

Privacy Risk Register

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 or not 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 (patient-level data unless otherwise stated)			
Name		N	
NHS number		N	
Address		N	
Postcode		N	
Date of birth		N	
Date of death		N	
Age		Y	Age at diagnosis (years) – case-mix variable for analysis
Sex		N	
Marital Status		N	

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]*
Gender		N	
Living Habits		N	
Professional Training / Awards		N	
Income / Financial / Tax Situation		N	
Email Address		N	**NATCAN contact database** Not collected for patients. Information held for extended provider teams only for administration of the audit – keeping teams informed about key audit dates and updates e.g data submission deadlines, publication of annual reports etc
Physical Description		N	
General Identifier e.g. Hospital No	N		
Home Phone Number	N		
Online Identifier e.g. IP Address/Event Logs	N		
Website Cookies	N		**NATCAN website** Collected on NATCAN 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	N		
Device Mobile Phone / Device IMEI No	N		
Location Data (Travel / GPS / GSM Data)	Y		
Device MAC Address (Wireless Network Interface)	N		
Sensitive Personal Data			
Physical / Mental Health or Condition	N		The de-identified linked extracts of data for the NATCAN include a wide range of patient, tumour and treatment characteristics More information about the NDRS datasets is provided here: https://www.ndrs.nhs.uk/
Sexual Life / Orientation	N		
Family / Lifestyle / Social Circumstance	N		

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]*
Offences Committed / Alleged to have Committed	N		
Criminal Proceedings / Outcomes / Sentence	N		
Education / Professional Training	N		
Employment / Career History	N		
Financial Affairs	N		
Religion or Other Beliefs	Y		
Trade Union membership		N	
Racial / Ethnic Origin	Y		Case-mix variable for analysis
Biometric Data (Fingerprints / Facial Recognition)		N	
Genetic Data		N	
Spare			
Spare			
Spare			

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 data flow to the NATCAN is de-identified - none of the datasets received by the NATCAN project team contain confidential patient identifiers. There is separation of identifiers and analysis datasets in the data flow.

All de-identified data extracts are stored on a password protected encrypted server at the RCSEng with restricted access to named analysts in the NATCAN project team. Data quality checking is performed by the NATCAN analysts and any issues, for example missing data, are escalated to the NATCAN data collection partners. Information about the quality standards of the information they collect can be found on their website.
https://www.ndrs.nhs.uk/
Key COSD Data Items 2023/2024 - National Cancer Audit Collaborating Centre (natcan.org.uk)

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 individuals rights
Individuals are clear about how their personal data is being used.	Privacy notice on NATCAN and RCS websites. Patient information FAQs on NATCAN website	See column to the left	https://www.rcseng.ac.uk/terms-and-conditions/ https://www.rcseng.ac.uk/privacy-policy/ UK IT Deployment Project Charter (natcan.org.uk) FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
Individuals can access information held about them	Privacy notice on NATCAN and RCS websites. Patient information FAQs and information on the NPCA data collection partners on the NPCA website	See column to the left	https://www.rcseng.ac.uk/terms-and-conditions/ https://www.rcseng.ac.uk/privacy-policy/ UK IT Deployment Project Charter (natcan.org.uk) FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
Request erasure (right to be forgotten) in certain circumstances, making clear that it	Privacy notice on NATCAN and RCS websites.	See column to the left	https://www.rcseng.ac.uk/terms-and-conditions/ https://www.rcseng.ac.uk/privacy-policy/ UK IT Deployment Project Charter (natcan.org.uk)

does not apply to an individual's health or care record, or for public health or scientific research purposes	Patient information FAQs and information on the NATCAN website		FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
Rectification of inaccurate information	Privacy notice on NATCAN and RCS websites. Patient information FAQs and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	https://www.rcseng.ac.uk/terms-and-conditions/ https://www.rcseng.ac.uk/privacy-policy/ UK IT Deployment Project Charter (natcan.org.uk) FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
Restriction of some processing	Privacy notice on NATCAN and RCS websites. Patient information FAQs and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	https://www.rcseng.ac.uk/terms-and-conditions/ https://www.rcseng.ac.uk/privacy-policy/ UK IT Deployment Project Charter (natcan.org.uk) FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
Object to processing undertaken on some legal bases	Privacy notice on NATCAN and RCS websites. Patient information FAQs and information on the NATCAN data collection partners on the	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)

	NATCAN website - includes information on patient opt out		
Complain to the Information Commissioner's Office; See column to the left	Not at present	See column to the left	
Withdraw consent at any time (if processing is based on consent)	Privacy notice on NATCAN and RCS websites. Patient information leaflet, FAQ and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
Data portability (if relevant)	N/A	See column to the left	
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Privacy notice on RCS website.	See column to the left	https://www.rcseng.ac.uk/terms-and-conditions/ https://www.rcseng.ac.uk/privacy-policy/ UK IT Deployment Project Charter (natcan.org.uk)
In which countries the data controller is processing their personal data. For data transfers outside the EU, a description of how the data will protected (e.g. the recipient is in an 'adequate' country / how a copy of the safeguards can be obtained.	Patient information FAQs NATCAN website. No personal data is transferred outside the EU.	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)

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?	Patient information FAQs and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
To know the purpose(s) for the processing of their information.	Patient information FAQs and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Patient information leaflets, FAQ and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
The source of the data (where the data were not collected from the data subject)	Patient information leaflets, FAQ and information on the NATCAN data collection partners on the NATCAN website - includes	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)

	information on patient opt out		
Categories of data being processed	Patient information leaflets, FAQ and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
Recipients or categories of recipients	Patient information leaflets, FAQ and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
The source of the personal data	Patient information leaflets, FAQ and information on the NATCAN data collection partners on the NATCAN website - includes information on patient opt out	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk) NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
To know the period for which their data will be stored (or the criteria	Patient information leaflets, FAQ and information on	See column to the left	FAQs - National Cancer Audit Collaborating Centre (natcan.org.uk)

used to determine that period)	the NATCAN data collection partners on the NATCAN website - includes information on patient opt out		NATCAN Information Governance and Privacy Policy - National Cancer Audit Collaborating Centre About NDRS - NDRS (digital.nhs.uk)
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	See column to the left	

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 regards 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 holds now and how many more records you anticipate receiving each year.

The number of records is to be determined, this section will be updated during the next review.

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 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 particular 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**
Risks to the individual for whom the NATCAN holds data								
Illegitimate access to de-identified patient-level data held by the NATCAN	1	3	3	**Y**	Ensure access to data is restricted to those who are authorised to do so	Only members of the NATCAN Project Team have access to the data held by the NATCAN, which is stored securely on an encrypted server	N/A	Dr. Julie Nossiter (JN)
Undesired modification of de-identified patient-level data held by the NATCAN	1	1	1	**Y**	Ensure access to data is restricted to those who are authorised to do so	Only members of the NATCAN Project Team have access to the data held by the NATCAN, which is stored securely on an encrypted server	N/A	JN

Disappearance of de-identified patient-level data held by the NATCAN	1	1	1	Y	Secure data back-ups	Data held by the NATCAN is stored securely on an encrypted server which is backed-up	N/A	JN
Re-identification of de-identified patient-level data held by the NATCAN	1	3	3	Y	There is no re-identification risk without human agency. Ensure access to data is restricted to those who are authorised to do so	Only members of the NATCAN Project Team have access to the data held by the NATCAN, which is stored securely on an encrypted server	N/A	JN
Corporate risks & compliance risks section								
Risks to the CEU, RCS								
Non-compliance with DPA	1	5	5	Y	Ensure NATCAN is compliant with DPA	Implement and follow DPA	In progress	JN
Illegitimate access to de-identified patient-level data held by the NATCAN	1	4	4	Y	Ensure access to data is restricted to those who are authorised to do so	Only members of the NATCAN Project Team have access to the data held by the NATCAN which is stored securely on an encrypted server	N/A	JN
Undesired modification of de-identified patient-level data held by the NATCAN	1	4	4	Y	Ensure access to data is restricted to those who are authorised to do so	Only members of the NATCAN Project Team have access to the data	N/A	JN

						held by the NATCAN, which is stored securely on an encrypted server		
Disappearance of de-identified patient-level data held by the NATCAN	1	4	4	Y	Secure data back-ups	Data held by the NATCAN is stored securely on an encrypted server which is backed-up	N/A	JN
Re-identification of de-identified patient-level data held by the NATCAN	1	4	4	Y	There is no re-identification risk without human agency. Ensure access to data is restricted to those who are authorised to do so	Only members of the NATCAN Project Team have access to the data held by the NATCAN, which is stored securely on an encrypted server	N/A	JN

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, send an updated version to your HQIP project manager and ensure that you incorporate any identified risks/issues to your risk/issue registers of the project contract review form.

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	**√**	**Page 2, version control**
Name of DPO	**Katarzyna Wieckowska**	k.wieckowska@dpocentre.com **Date completed: 26/03/2024**
Name and role of person approving completion of DPIA form. This must not be the same person that completes the form.		
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?		
Does it include a systematic description of the proposed processing operation and its purpose?	**√**	
Does it include the nature, scope, context and purposes of the processing	**√**	
Does it include personal data, recipients and period for which the personal data will be stored are recorded		
Does it include the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels)	**√**	**Page 13**
Does the DPIA explain how each individual's rights are Managed? See section on individuals rights	**√**	See section on individuals rights
Are safeguards in place surrounding international transfer? See section on sending information outside the EEA	**N/A**	**N/A**

Was consultation of the document carried out and with whom?	**DPO**	**Completed 26/03/2024**
Organisations ICO registration number	**Z5948910**	**Royal College of Surgeons of England | ICO**
Organisations ICO registration expiry date	**24 October 2026**	**Royal College of Surgeons of England | ICO**
Version number of the DPIA you are submitting		
Date completed		

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 / HQIP / NHSE, breach of confidentiality/loss of personal sensitive data or up to 1000 records</td></tr>
</table>
</td></tr>
</table>

	5	Catastrophic	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 / HQIP / NHSE, serious breach of confidentiality/loss of personal sensitive data >1000 records involved
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?		