Data Protection Impact Assessment for the Epilepsy12 Audit

Document control:

	Name and role	Contact details
Document Completed by	Epilepsy12 Project Manager	epilepsy12@rcpch.ac.uk 020 7092 6168
Data Protection Officer name	Head of Information Governance	Information.Governance@rcpch.ac.uk 020 7092 6000
Document approved by (this should not be the same person that completes the form).	Head of Information Governance	Information.Governance@rcpch.ac.uk 020 7092 6000
Organisation's ICO registration number can be found at https://ico.org.uk/esdwebpages/search	Z5143673	

Date Completed	Version	Summary of changes
30/04/2018	0.1	Epilepsy12 Project Manager first draft
04/05/2018	0.2	Information Governance Manager comments
04/05/2018	0.3	Information Governance Manager further comments
10/05/2018	0.4	Information Governance Manager further comments
11/05/2018	0.5	Information Governance Manager suggested risk addition and approval
09/07/2018	0.6	Information Governance Manager added corporate risks
24/04/2020	1.1	Review following 1st cohort of patients. Added information on new: • capacity for Trusts to download their data. • collection of genetic causes of epilepsy. • NHS national opt-out from September 2020

31/03/2022	1.2	• Added project extension to Round 4 • Added intent to collect ethnicity data
05/07/2023	2	Change of system provider – substantial change
09/11/2023	2.1	Epilepsy12 Project Manager – finalised updates and changes made by IG consultant **Data Privacy Simplified and BJM IG Privacy**
22/10/2024	2.2	Updated as storage with NetSolving terminated
21/03/2025	2.3	Add Jersey data

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		
2	Does your project involve any sensitive information or information of a highly personal nature?	Y		
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.	Y		
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		
5.	Does your project match data or combine datasets from different sources?	Y		
6.	Does your project collect personal data from a source other than the individual without providing them with privacy notice ('invisible processing')?	N		
7.	Does your project process data that might endanger the individual's physical health or safety in the event of a security breach?	N		
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?	N		

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 UK GDPR (UK General Data Protection Regulation) since the 25th May 2018 and the 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.

Post planning stage and agreement of project methodology but prior to the launch of the clinical audit phase of the project. Reviews and revisions have since taken place following the first clinical audit phase, and at the start of an additional contract period.

DPIA update March 2025 updated to include the processing of Jersey data.

DPIA update October 2024, the Epilepsy 12 platform has been fully migrated from NetSolving to Azure hosted open-source database managed by RCPCH. Any remaining data held by NetSolving has been securely destroyed.

DPIA update July 2023, reviewed during the development work to move system from NetSolving to Azure hosted open-source database and prior to its move. As part of this move the datasets that are collected have been reviewed with some previously unused data items being removed and additional specific dataset relating to mental health, neurological conditions and learning disabilities added. Additional capability is being developed to allow for API upload of data from participating organisations to further reduce risk of transcription errors and enable efficiencies. CAG amendment sought support for the RCPCH (with Microsoft Azure as a sub processor), to administer the Epilepsy12

Epilepsy12 was established in 2009 and has the continued aim of helping epilepsy services, and those who commission health services, to measure and improve the quality of care for children and young people with seizures and epilepsies.

The audit processes data captured on the structure of epilepsy services and on the patient care given by paediatric epilepsy services within Health Boards in Wales and Trusts in England. This is used to identify areas for quality improvement in relation to the delivery and outcomes of care.

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.

RCPCH Data Protection Officer and Head of Information Governance (09 April 2018, 30 April 2018, 24 April 2020, 13 April 2022, 16/11/2023, 21/03/2025)

Consultation in relation to the privacy risks of the Epilepsy12 Round 3 methodology and fair processing materials was undertaken with members of both the Epilepsy12 Project Board and Methodology & Dataset Group (September 2017 to March 2022). This was similarly undertaken for the Round 4 methodology (April 2022 to March 2025).

Please see below the full list of Epilepsy12 stakeholders that are represented within the Project Board and Methodology and Dataset group. Patient organisations are indicated in bold:

- British Paediatric Neurology Association, British Society for Clinical Neurophysiology, **Epilepsy Action**, Healthcare Quality Improvement Partnership, OPEN UK, RCPCH Epilepsy12 Manager, RCPCH Epilepsy12 Data Analyst, RCPCH Epilepsy12 Co-ordinator, Statistics consultant, RCPCH Head of Audits, RCPCH Senior Data Analysts, RCPCH Audit Administrator, , RCPCH CYP Engagement Manager, Royal College of Nursing, Epilepsy Specialist Nurses Association, **Young Epilepsy,** NHS England, Welsh Government

Update 05/07/2023: Changes of System Provider
The system is moving into a RCPCH controlled Azure tenant. An external Data Protection and Cyber consultancy was engaged (Data Privacy Simplified and BJM IG Privacy) to support review and risk identification and is contributing to this document.

Update 19/10/2023: CAG amendment submission
On the 30/08/2023 an amendment submission was sent to the Health Research Authority Confidentiality Advisory Group (HRA CAG), CAG reference 17/CAG/0184. This was fully supported and a fully supported outcome letter was issued to RCPCH on 19/10/2023. This has been published on the Epilepsy12 website and on the new platform**.**

Update 22/10/2024: Migration to RCPCH database complete

The migration to the RCPCH database from NetSolving has now been completed and NetSolving have been notified of contract termination and will destroy the data and provide written confirmation of secure destruction.

Update 31/03/2025: Represneatives from NHS Engalnd and Welsh Government invited to the Project Board. Jersey colleagues will also be invited once a represenative is identified.

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.

We intend to publish the full reviewed DPIA report for the project on the Epilepsy12 web pages of the RCPCH website (www.rcpch.ac.uk/epilepsy12) by December 2023. This will also be published on the 'guidance' page on the data platform: https://epilepsy12.rcpch.tech/ .

The updated DPIA is published on the Epilepsy 12 webpages of the RCPCH website.

March 2025- the updated DPIA will be published on the RCPCH website on the Epilepsy 12 webpages.

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.

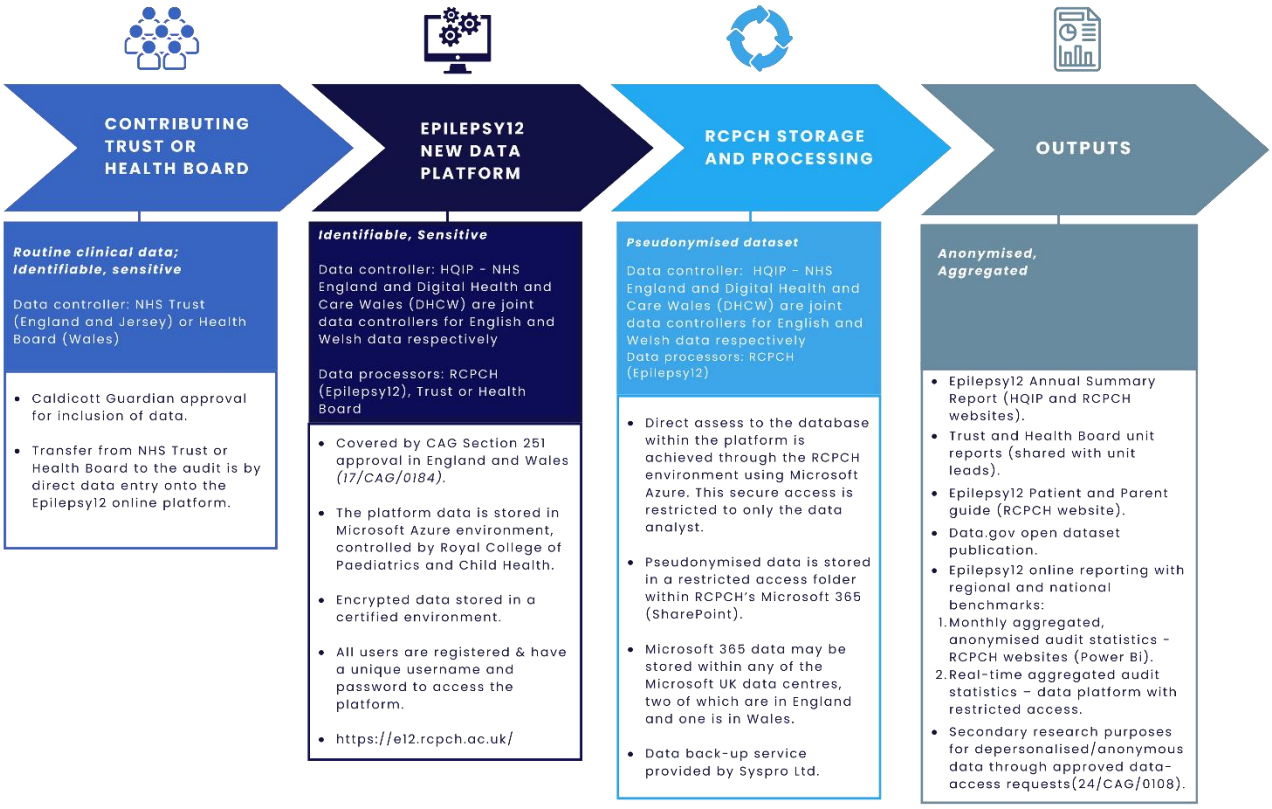
Processing activity description	**Type of data involved**	**Data flow**	**Controller/processor**
Clinical data entered by paediatric epilepsy services within NHS Health Boards and Trusts via the secure Epilepsy12 data platform.	Personal data (identifiable) and special category data relating to children	NHS Health Boards and Trusts enter data onto the secure Epilepsy12 data platform. NHS Health Boards and Trusts may also download their data. This creates an encrypted, password-protect zip file. Options prompt users to include the least amount of pseudonymised personal data in their download, based on their needs. will not have download capability following data upload.	Data controller: NHS Health Boards in Wales, NHS Trusts in England and Jersey Hospital in Jersey
Clinical audit data stored on the Epilepsy12 data platform servers which are maintained in house by RCPCH and hosted within their Azure Tennent.	Personal data (identifiable) and special category data relating to children	None.	Data processors: RCPCH Data sub-processor: Microsoft Data controller: HQIP (NHS England and Digital Health and Care Wales (DHCW) are joint data controller for English and Welsh data respectively)
Epilepsy12 data downloaded to RCPCH servers for storage prior to analysis. The patient identifiable dataset will be pseudonymised before download.	Pseudonymised/ limited access de-identified.	From Epilepsy12 platform servers to a restricted folder on the RCPCH servers.	Data processor: RCPCH Data sub-processor: Microsoft Data controller: HQIP (NHS England and Digital Health and Care Wales (DHCW) are joint data controller for English and Welsh data respectively)
Re-extracted, cleaned data used to develop tables and statistical outputs and reports. Health Board/Trust, NHS E ICB and region, and	Pseudonymised/ limited access de-identified becomes anonymised and aggregated data	Epilepsy12 project team produces and publishes report outputs on the Epilepsy12 website. Trust/Health Board reports, contain patient	Data processor: RCPCH Data sub-processor: Microsoft Data controller: HQIP (NHS England and Digital Health and Care Wales

OPEN UK regional network level results also publicly accessible on Epilepsy12 and data.gov.uk websites.		identifiable information, are shared with designated leads only and are not publicly available. Project team provides NHS England with aggregated and anonymised data outputs on specified metrics.	(DHCW) are joint data controller for English and Welsh data respectively)
Data is extracted from the platform, cleaned, and analysed to develop datasets and statistical outputs for Data Access Requests, where these are approved by HQIP (the data controller).	Depending on the nature of the request and type of data access approved by HQIP (with the least amount of personal data possible included in any instance): • Personal data (identifiable) • Pseudonymised data • De-identified aggregated data	Epilepsy12 project team produces and securely shares data access outputs via approved means and for a specified time period.	Data processor: RCPCH Data sub-processor: Individual or entity approved for data access Data controller: HQIP (NHS England and Digital Health and Care Wales (DHCW) are joint data controller for English and Welsh data respectively)

Data flow Diagram

EPILEPSY12

EXTERNAL DATA FLOW DIAGRAM



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).

Data is being transferred between Jersey and the UK for the purposes of including Jersey within the audit. The UK deems Jersey adequate and Jersey Office of the Information Commissioner has deemed UK adequate (adequacy decision)

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			
Name	N		First name and Surname data fields will be captured to aid local provider patient monitoring and clinical improvement activity only. Data collection for each child is ongoing to allow longitudinal data entry and analysis. Retaining patient names will help ensure that ongoing data entry is aligned to the correct child. These details would not be extracted from the system or included in analysis by the central project team.
NHS number (England and Wales) or URN number (Jersey)	N		The NHS number is required as this will be a unique identifier for the patient on the system which will allow for a cross check at the point of registration of whether the particular patient has already been entered into the audit, improving data quality. It will also allow for linkage with other NHS data (if required) and with the NHS national patient data opt out registry. This will in turn then allow for report and trend analysis.
Address	N		Full home address will not be collected.
Postcode	Y		Home postcode will be required to analyse deprivation and to produce an atlas of variation for care processes, service provision and outcomes. This data will be transformed into a Lower-layer Super Output Area (LSOA) automatically by the system. The project team will only download and analyse LSOA outputs.
Date of birth	Y		Date of birth is required for patient inclusion criteria and for the comparative assessment of outcomes and treatment efficacy by age. This data will be transformed automatically by the system to provide age at first assessment. The project team will only download and analyse this data and not full DOB.
Date of death	N		This data is no longer collected.

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]*
Age	Y		Age at first assessment is calculated from date of birth, age is required for patient inclusion criteria and for the comparative assessment of outcomes and treatment efficacy by age. Age is also relevant to the prescription of certain Anti-epileptic Drug (AEDs).
Sex	Y		Sex will be required in order to validate the appearance of relevant data fields within the system such as those related to the discussion of fetal risk with females currently receiving sodium valproate treatment. This is also required for the comparative assessment of outcomes and treatment efficacy by sex.
Marital Status	N		This data is not collected.
Gender	Y		Gender will be required in order to validate the appearance of relevant data fields within the system such as those related to the discussion of fetal risk with females currently receiving sodium valproate treatment. This is also required for the comparative assessment of outcomes and treatment efficacy/equality by gender.
Living Habits	N		This data is not collected.
Professional Training / Awards	N		This data is not collected.
Income / Financial / Tax Situation	N		This data is not collected.
Email Address	Y		Patient email addresses are not collected. Clinician email addresses are required to securely log in to the Epilepsy12 data platform system.
Physical Description	N		This data is not collected.
General Identifier e.g. Hospital No	N		This data is not collected.
Home Phone Number	N		Patient phone numbers are not collected. Work phone number is recorded for clinicians registered to use the Epilepsy12 data platform system; in order to assist the project team to provide technical support for the platform only.
Online Identifier e.g. IP Address/Event Logs	N		No patient online identifiers are collected. Online identifiers for clinicians and platform users will be logged to monitor activity. This will only be accessed if required for an investigation into an error/breach etc.
Website Cookies	N		This data is not collected.
Mobile Phone / Device No	N		This data is not collected.
Device Mobile Phone / Device IMEI No	N		This data is not collected.
Location Data (Travel / GPS / GSM Data)	N		This data is not collected.
Device MAC Address (Wireless Network Interface)	N		This data is not collected.

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]*
Sensitive Personal Data			
Physical / Mental Health or Condition	Y		Details of individual patient condition and care are required for the comparative assessment of outcomes and treatment efficacy and to aid local provider patient monitoring and clinical improvement activities.
Sexual Life / Orientation	Y		If a prescription of Sodium Valproate medication is entered into the audit, data is collected (yes/ no) whether there was a discussion with the patient about of the risks of valproate use during pregnancy. This is to audit whether the standards of care in relation to the use of sodium valproate medications are being met.
Family / Lifestyle / Social Circumstance	Y		Patient home postcode is used to reference to the Indices of Multiple Deprivation for England and Wales. This is required to analyse deprivation and to assess unwarranted variation/health inequalities for care processes, service provision and outcomes.
Offences Committed / Alleged to have Committed	N		This data is not collected.
Criminal Proceedings / Outcomes / Sentence	N		This data is not collected.
Education / Professional Training	N		This data is not collected.
Employment / Career History	N		This data is not collected.
Financial Affairs	N		This data is not collected.
Religion or Other Beliefs	N		This data is not collected.
Trade Union membership	N		This data is not collected.
Racial / Ethnic Origin	Y		Patient ethnic origin data is required to analyse potential unwarranted variation/health inequalities for care processes, service provision and outcomes.
Biometric Data (Fingerprints / Facial Recognition)	N		This data is not collected.
Genetic Data	Y		We collect genetic and chromosomal causes of epilepsy, where present. Details of individual patient condition and care are required for the comparative assessment of outcomes and treatment efficacy and to aid local provider patient monitoring and clinical improvement activities.

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.

System validation checks are in place to minimise data entry error, for example, date of first assessment cannot be before the DOB. Additional data quality and validation checks will be carried out on the data by the RCPCH Epilepsy12 project team prior to analysis for the preparation of national and regional reports.

Real-time feedback on performance metrics will allow Health Boards and Trusts to check the quality of data and amend any data entry errors before submitting audit data for annual analyses. Quarterly and monthly reporting will also facilitate quality assurance in the same way.

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.	Related details will be included in the public information/fair processing leaflet and supporting materials. The privacy notice will be targeted to the appropriate audience.	Published on our website, distributed electronically to participating registered Health Boards/Trusts.	**Why are hospitals and clinics taking part in Epilepsy12?** We want to get better at looking after children and young people who have epilepsy. Hospitals and clinics can help by collecting important information on the care that they provide to their patients. The RCPCH will look at this information and let teams know where they are doing well and what they need to get better at. The RCPCH will also tell hospitals and clinics how they are doing, compared with others who are taking part. All hospitals and clinics in England, Jersey and Wales that care for children and young people with epilepsy should take part in Epilepsy12.

Individuals can access information held about them	Related details will be included in the public information/fair processing leaflet and supporting materials.	If a patient or parent makes a subject access request (SAR) the RCPCH will only respond where we are the data controller of the data. If we are the data processor, we will forward any requests for access to the relevant data controller and write to the individual to advise them that we have forwarded on their request.	**What rights do I have?** If you have any questions or would like to make any rights requests, please contact your unit directly. For the data we collect for Epilepsy12, you have the following rights: Right of access: The personal data we hold about you is provided by your unit. We can let you know which categories of data we collect, depending on the type of submission, but you will need to contact your unit directly for a copy of the information as they are data controllers of your patient record.
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	Related details will be included in the public information/fair processing leaflet and supporting materials and in instructions for staff members within the RCPCH.	Forward the request to the data controller, HQIP.	Right to Erasure and Right to Object: The right of erasure does not apply to this audit because your data is being processed for the purposes of performing a task in the public interest, which in this case is for ensuring high standards of quality and safety health care. However, if you want to opt out of future audit rounds, please let your unit know and they will remove you from the submission so that we don't receive the data. Alternatively, you can contact the Epilepsy12 team directly at epilepsy12@rcpch.ac.uk , and we will ensure that your personal identifiers are removed from our database.
Rectification of inaccurate information	Related details will be included in the public information/fair processing leaflet and supporting materials.	Forward the request to the data controller, HQIP.	Right to rectification of inaccurate data: Any requests to amend or update your personal data should be sent to your unit as data controller. If we receive any requests, we will forward these to the Trust/Health Board.
Restriction of some processing	Related details will be included in the public information/fair processing leaflet and supporting materials.	Forward the request to the data controller, HQIP.	Right to restriction: Any requests for restriction of processing should be sent to your Trust/Health Boards and they will inform us where applicable.

Object to processing undertaken on some legal bases	Related details will be included in the public information/fair processing leaflet and supporting materials. Epilepsy12 were granted an exemption to applying the NHS England national-opt out policy on 10 January 2023. Details will be included in public information, and for Trusts and Health Boards using the Epilepsy12 website or data platform.	Forward the request to the data controller, HQIP.	**What if I don't want my information to be collected for Epilepsy12?** If you do not want your personal information to be collected for the Epilepsy12 audit, please let your paediatric epilepsy team know and they will remove you from the submission so that we don't receive the data. Alternatively, you can contact the Epilepsy12 team directly at epilepsy12@rcpch.ac.uk and we will ensure that your personal identifiers are removed from our database. In England, the National Data Opt-Out service allows patients to opt out of their information being used for research or planning purposes. The National Opt-Out service does not remove your information from Epilepsy12. In England, the National Data Opt-Out (NDO) service allows patients aged 13 or over (or those with parental responsibility for patients under 13) to opt out of their information being used for purposes beyond their direct care. The Secretary of State for Health and Social Care, having considered the advice from the Health Research Authority Confidentiality Advisory Group, has decided that the NDO will not be applied to Epilepsy12. This is because applying the NDO would introduce biases to the data and make it difficult to monitor care safety and quality and because of the importance of the data collection for improving patient care. Personal data collected by Epilepsy12 is not for research; it is processed to make sure epilepsy care is being provided safely and that health services meet national standards for care quality. **Opting Out in Jersey** To exercise your right to opt-out of your data being used for National Audit and research, you can email the Clinical Audit team at HSSClinicalAuditDepartment@health.gov.je. You can also request that the processing of your data for national audit purposes is restricted through the online form found at your personal data rights. Data of Jersey

			patients who have opted out will be excluded from data flows to England.
Complain to the Information Commissioner's Office;	Related details will be included in the public information/fair processing leaflet and supporting materials.	Forward the request to the data controller, HQIP.	**Who should I contact if I need more information?** If you would like more information about Epilepsy12, please contact epilepsy12@rcpch.ac.uk or call us on 020 7092 6168. You can also contact the College's data protection officer for queries about how the college process personal data: information.governance@rcpch.ac.uk. If you have any further questions or concerns about how your information is being shared for the purposes of the audit, please first contact your hospital team. HQIP are the joint data controllers with NHS England and Digital Health and Care Wales for the England and Wales elements of the audit respectively. HQIP can also be

			contacted if you have any questions or concerns about how your information is being used for the audit: data.protection@hqip.org.uk. You do also have the right to lodge a complaint with the Information Commissioner's Officer (ICO) at casework@ico.org.uk, if you have concerns about the way your/your child's personal data is being handled. If you live in Jersey you can complain to the Jersey Office of the Information Commissioner.
Withdraw consent at any time (if processing is based on consent)	Not applicable.	Not applicable.	Not applicable.
Data portability (if relevant)	Not applicable.	Not applicable. Data is not collected directly from the data subject, part of a contract or based on consent.	Not applicable.
Individual knows the identity and contact details of the data controller and the data controllers data protection officer	Related details will be included in the public information/fair processing leaflet and supporting materials.	Forward the request to the data controller, HQIP.	**Who should I contact if I need more information?** If you would like more information about Epilepsy12, please contact epilepsy12@rcpch.ac.uk or call us on 020 7092 6168. You can also contact the College's data protection officer for queries about how the college process personal data: information.governance@rcpch.ac.uk. If you have any further questions or concerns about how your information is being shared for the purposes of the audit, please first contact your hospital team. HQIP are the joint data controllers with NHS England and Digital Health and Care Wales for the England and Wales elements of the audit respectively. HQIP can also be contacted if you have any questions or concerns about how your information is being used for the audit: data.protection@hqip.org.uk. You do also have the right to lodge a complaint with the Information Commissioner's Officer (ICO) at casework@ico.org.uk, if you have concerns

			about the way your/your child's personal data is being handled. If you live in the UK, you do also have the right to lodge a complaint with the ICO if you have concerns about the way your/your child's personal data is being handled: casework@ico.org.uk. If you live in Jersey you can complain to the Jersey Office of the Information Commissioner.
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.	Related details will be included in the public information/fair processing leaflet and supporting materials.	Published on our website, distributed electronically to participating registered Health Boards/Trusts.	Data collected are held on secure servers which are hosted within the EU. Units in Jersey will share personal data with the Epilepsey12 audit which is based in the UK. The UK is deemed adequate by the EU, they are also deemed adequate by the Jersey Office of the Information Commissioner, so no further steps are required to ensure the transfer of your personal data between the UK and Jersey.
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?	Related details will be included in the public information/fair processing leaflet and supporting materials.	Published on our website, distributed electronically to participating registered Health Boards/Trusts. We are processing under schedule 6(e) and schedule 9(i) of GDPR and have section 251 CAG approval (reference: 17/CAG/0184)	**Why didn't anyone ask me if they could collect my personal information for Epilepsy12?** The legal reason is that it is in the public interest for the RCPCH Epilepsy12 project to use your personal data. Epilepsy12 has section 251 approval to collect patient identifiable data in England, Jersey and Wales without explicit patient consent as it improves epilepsy care for children. To find out more about section 251 approval, visit the Health Research Authority website. Processing is permitted under the UK General Data Protection Regulation (GDPR) on the following legal bases: Article 6 (1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is justified through commissioning arrangements which link back to NHS England, Jersey and the Welsh Government. Article 9 (2) (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against

			serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. This is justified as Epilepsy12 aims to drive improvements in the quality and safety of care and to improve outcomes for patients. This means the audit does not need to ask permissions from everybody. However, we take your privacy seriously, so we offer you the option to opt out if you do not want to take part. The section below 'What rights do I have?' explains how you can do this and more about your rights. In Jersey, processing is permitted under the Data Protection (Jersey) law 2018 under the following legal bases: - Public interest under the common law of duty of confidentiality
To know the purpose(s) for the processing of their information.	Related details will be included in the public information/fair processing leaflet and supporting materials.	Published on our website, distributed electronically to participating registered Health Boards/Trusts.	**What is Epilepsy12?** Epilepsy12 is an important national project which helps epilepsy services to measure and improve the quality of care for children and young people with epilepsies. The Royal College of Paediatrics and Child Health (RCPCH) are commissioned by the Healthcare Quality Improvement Partnership (HQIP), as part of their National Clinical Audit and Patient Outcomes Programme (NCAPOP). This means that we were chosen to run Epilepsy12 on behalf of NHS England, Jersey and the Welsh government. **Why are hospitals and clinics taking part in Epilepsy12?** We want to get better at looking after children and young people who have epilepsy. Hospitals and clinics can help by collecting important information on the care that they provide to their patients. The RCPCH will look at this information and let teams know where they are doing well and what they need to get better at. The RCPCH will also tell hospitals and clinics how they

			are doing, compared with others who are taking part. All hospitals and clinics in England, Jersey and Wales that care for children and young people with epilepsy should take part in Epilepsy12. **What information does Epilepsy12 collect?** Epilepsy12 wants to find out how hospitals and clinics decide if a child has epilepsy and how they look after them if they do. For example, we collect information on the types of medicine that children with epilepsy receive, and the doctors and nurses that look after them. You can see a list of all the information that Epilepsy12 collects on our website: www.rcpch.ac.uk/epilepsy12. The private information, known as personal data, collected by Epilepsy12 includes patient's name, date of birth, gender, home postcode and something called their "NHS" number. NHS numbers help hospitals and clinics to identify patients. Your hospital or clinic already collects this information, so this isn't something new for Epilepsy12.
Whether the provision of personal data is part of a statutory obligation and possible consequences of failing to provide the personal data.	Not applicable	Not applicable- there is no statutory obligation for patients/parents to provide their data to the Epilepsy12 audit.	Not applicable.
The source of the data (where the data were not collected from the data subject)	Related details will be included in the public information/fair processing leaflet and supporting materials.	Published on our website, distributed electronically to participating registered Health Boards/Trusts.	**What information does Epilepsy12 collect?** Epilepsy12 wants to find out how hospitals and clinics decide if a child has epilepsy and how they look after them if they do. For example, we collect information on the types of medicine that children with epilepsy receive, and the doctors and nurses that look after them. You can see a list of all the information that Epilepsy12 collects on our website: www.rcpch.ac.uk/epilepsy12. The private information, known as personal data, collected by Epilepsy12 includes patient's name, date of birth, gender, home postcode and something called their "NHS" number. NHS numbers help hospitals and clinics to identify patients. Your hospital or

			clinic already collects this information, so this isn't something new for Epilepsy12. URN numbers are used in Jersey in place of NHS numbers.
Categories of data being processed	Related details will be included in the public information/fair processing leaflet and supporting materials.	Published on our website, distributed electronically to participating registered Health Boards/Trusts.	**What information does Epilepsy12 collect?** The private information, known as personal data, collected by Epilepsy12 includes patient's name, date of birth, gender, home postcode and something called their "NHS" number. NHS numbers help hospitals and clinics to identify patients. Your hospital or clinic already collects this information, so this isn't something new for Epilepsy12. URN numbers are used in Jersey in place of NHS numbers.
Recipients or categories of recipients	Related details will be included in the public information/fair processing leaflet and supporting materials.	We currently don't share data with anyone. We may seek to link to HES, ONS, PEDW data in the future via the NHS number.	**What happens to the private information?** The RCPCH will not send your private information to anyone else unless they have permission to do so. If Epilepsy12 information is needed for other projects to compare services in England and Wales, they will need permission from HQIP. For HQIP to approve this request, the project must show that they follow the strict data protection policies described in HQIP's guidance to applicants, and must aim to improve care for children with epilepsy. Data will only ever be shared in a pseudonymised format, which is where information that could identify you is removed or replaced (unless the requesting institution has its own legal basis for holding patient identifiable data).
The source of the personal data	Related details will be included in the public information/fair processing leaflet and supporting materials.	Published on our website, distributed electronically to participating registered Health Boards/Trusts.	**What happens to the private information?** Epilepsy services enter your information collected for Epilepsy12 onto a safe and secure website. This website can only be accessed by staff working in hospitals and clinics who have the right access permissions, or those working on the Epilepsy12 project at the RCPCH.
To know the period for which their data will be stored (or the criteria used to determine that period)	Related details will be included in the public information/fair processing leaflet and supporting materials.	Published on our website, distributed electronically to participating registered Health Boards/Trusts.	**How long do you keep my personal information for?** The Epilepsy12 team at the RCPCH acts as the data processor on behalf of the Healthcare Quality Improvement Partnership (HQIP) who are data controller for the audit. NHS England and Digital Health and Care Wales, who are also the joint data controllers for Epilepsy12 data for England and Wales. The RCPCH will hold your information for as long as it is

			commissioned by HQIP to deliver the Epilepsy12 audit. All data will be deleted or transferred back to HQIP within two weeks of the end of our contract.
The existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on data subjects (if applicable)	Not applicable.	Not applicable.	Not applicable.

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.

Considering previous cohort, it is anticipated that data for around 5,000 patients newly diagnosed with epilepsy will be added to the Epilepsy12 data platform each year.

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**
Illegitimate access, undesired modification and disappearance of data	1	5	5	**Reduced**	The Epilepsy12 data capture system has regular database backups which will be carried out as per planned schedules agreed with the system developers. These back-ups will be stored securely at an alternate site which conform to full Information Security and Network Security Policies. **The system is developed within an open-source repository that employs automated code and dependency**	As below, adequate validation and security checks are in place to ensure data is correctly exported/imported and safely transferred between the platforms. Adequate technical measures have been put in place to reduce the risk of a security incident by balancing the type of data being processed against the technical solutions available. If there is an	Already in place	RCPCH, Microsoft

					scanning techniques and is open to peer review. **Patient identifiable information that is entered onto the Epilepsy12 data platform is stored within a database hosted by RCPCH within their Microsoft Azure Tennent. Only specified and authorised individuals at RCPCH have access to the submitted data to be able to support the platform and access data to process, pseudonymise and apply analysis.** **All methods of data in transit is secured using TLS 1.2, sensitive personal data is encrypted at rest using AES 256 bit encryption.** **Internal firewalls and cloud-based security products (Azure) are used to enhance the defence in depth strategy. With**	incident, staff have received appropriate training and there is an appropriate procedure in place to contain the risk.		

					anomalous behaviour and threat prevention alerting enabled and monitored. **Access to the Epilepsy12 platform is restricted to authorised individuals with multifactor authentication or API to enable data submission.** For data processing, pseudonymised patient information is downloaded from the Epilepsy12 data platform server to the College server. Any identifying characteristics of data are automatically replaced with a pseudonym (a value which does not allow the data subject to be directly identified) priori to download. Pseudonymisation differs from anonymisation because it only provides a limited protection for the identity of data subjects as it still allows identification using indirect			

					means (e.g. by keeping a separate file of NHS numbers and their corresponding pseudocodes applied prior to analysis). The download function can only be performed by authorised RCPCH-based Epilepsy12 Project Team members via a dedicated login and password access to site administrator rights of access to the data platform. Once the data is downloaded from the Epilepsy12 data platform server, it is saved in a restricted access folder on RCPCH servers which can only be accessed by the Epilepsy12 project team members. The management of the Epilepsy12 data on the RCPCH servers will conform to the Access Controls set out within the RCPCH Information Security Policy and Data			

					Protection and Confidentiality Policy. This controls state that network security control shall be protected and managed by Internet Firewall. All Internet Traffic shall be virus checked, anti-spam checked and protected from intrusion (main common attack vectors). All staff handling identifiable data will undertake mandatory training on Data Protection and Information security, and may be asked to complete advanced training.			
Duplicated copies of the same information stored in two different places	2	2	4	**Reduced**	The RCPCH Epilepsy12 Project Team have a data cleaning and validation procedure in place to manage this and will review the validation procedure on a regular basis. Checks on the data platform prevent duplicate patient registrations (validated	Removes duplicate records, holds a master database from which data are analysed and queried.	In place	Epilepsy12 Project Team / RCPCH DPO

					against NHS number) Versions of the dataset are stored on RCPCH servers (in addition to the main version stored within Microsoft Azure). This is to ensure a copy of the data as they were at the time of analysis – this is to ensure an audit trail for published results. The stored reference copies are pseudonymised.			
Inadequate data sharing agreements in place when sharing information	2	3	6	**Eliminated**	All new data sharing agreements will be reviewed by the RCPCH Data Protection Officer and will be subject to the HQIP Data Access Request process. The RCPCH Epilepsy12 project team will have informed subjects about possible data linkage via the project privacy notice, and the RCPCH Data Protection Officer will check that the RCPCH has legal grounds for data sharing and section 251	To ensure that the DSA is fit for purpose and to obtain approval from HQIP as the Data Controller via its Data Access Request Group (DARG).	As and when necessary	Epilepsy12 Project Team / RCPCH DPO/ HQIP DARG

					approval if necessary. The project team will minimise the amount of personal data being shared and will consult with the RCPCH Data Protection Officer to ensure appropriate agreements are in place to share the data and that a common retention is agreed for the data and that it would be shared by secure means only.			
Inappropriate security on the system holding the data, including data being moved outside the EU.	1	5	5	**Eliminated**	Patient identifiable information that is entered onto the Epilepsy12 data platform will be stored within the RCPCH managed Azure infrastructure. For data processing, pseudonymised patient information will be downloaded from the Epilepsy12 data platform server to the College server. Any identifying characteristics of data are automatically replaced with a pseudonym (a	Reduces risk of data breach.	Already in place	RCPCH staff, Epilepsy12 project team

					value which does not allow the data subject to be directly identified) priori to download. Pseudonymisation differs from anonymisation because it only provides a limited protection for the identity of data subjects as it still allows identification using indirect means (e.g. by keeping a separate file of NHS numbers and their corresponding pseudocodes applied prior to analysis). The download function can only be performed by authorised RCPCH-based Epilepsy12 Project Team members via a dedicated login and password access to site administrator rights of access to the data platform. Once the data is downloaded from the Epilepsy12 data platform server, it is saved in a restricted access folder on RCPCH servers which			

					can only be accessed by the Epilepsy12 project team members. The management of the Epilepsy12 data on the RCPCH servers will conform to the Access Controls set out within the RCPCH Information Security Policy and Data Protection and Confidentiality Policy. This controls state that network security control shall be protected and managed by Internet Firewall. All Internet Traffic shall be virus checked, anti-spam checked and protected from intrusion (main common attack vectors). All staff handling identifiable data will undertake mandatory training on Data Protection and Information security, and may be asked to complete advanced training. Jersey- UK deeems Jersey			

					adequate and Jersey Office of the Information Commissioner has deemed UK adequate (adequacy decision)			
Data collection seen as intrusive by individuals due to the opt out, rather than consent approach.	2	2	4	**Reduced**	Public information leaflet and supporting materials include information required by GDPR. This will provide information for patients and parents on how they can opt out of their data being used in the audit. It will clearly explain the purpose of processing the data and the legal justification.	Communicates the purpose and legal basis for processing data.	In place	Epilepsy12 project team
System for opt out is not robust enough	2	3	6	**Reduced**	Epilepy12 has processes in place which provide the ability to record and honour any objections to the collection and processing of patient data. The Epilepsy12 fair processing materials and privacy notices comply with new GDPR requirements in relation to fair and lawful processing and have been reviewed and approved by the	The process ensures that patients and parents have a clear and effective way of exercising their right to opt out of participation in the audit which is underpinned by effective functions within the Epilepsy12	Epilepsy12 specific opt out in place. NHS national guidance will apply from 31 July 2022	Epilepsy12 project team

					RCPCH Information Governance Manager. The notices clearly explain to patients and parents the process for notifying their paediatric service directly and/or the RCPCH (by phone only in the case of the RCPCH) of any objections to the collection and use of their personal data for the purpose of Epilepsy12. Patients/parents will also be provided with details on the project privacy notice of their rights under data protection legislation, including how to opt out. Epilepsy12 have received an exemption to applying the NHS England National data opt out (NDO). As a results NDO patients are being registered onto the platform. Patients and families can still opt-out of Epilepsy12 specifically, and	data platform.		

					can do this by contacting their clinical team or the RCPCH as above. Patients opting out in this way will not have any data entered onto the platform in the first instance. If already registered, Health Boards/Trust designated leads can delete their record from the system, or request the Epilepsy12 project team to do so. The deletion will be recorded in the activity log. Jersey patients can opt out by either emailing the clinical audit team HSSClinicalAuditDepartment@health.gov.je or request restriction via the online form provided by Jersey Government: https://www.gov.je/Government/dataprotection/Pages/ChangingPersonalData.aspx. This is explained in the privacy notice.			
Future changes to the way data is used or shared. This	2	3	6	**Accepted**	Processes and guidance will be reviewed on a	Ensures timely review of	NA	Epilepsy12 Proje

may include the merger of datasets which may result in a wider dataset than individuals would expect.					regular basis and with any change to the project methodology. Changes are reviewed by the audit Methodology and Dataset Group; with changes to data processing/flow /items also reviewed by HQIP and CAG Section 251 approval where these reviews are required. If we are considering merging or linking datasets, we will first talk to the DPO about the GDPR implications and whether we need to make any changes to the privacy notice, or reconsider our legal grounds for processing.	communication and processes if there is a change in the project.		ct Team / RCPCH DPO
Knowing when the data should be deleted	2	2	4	**Accepted**	The retention period of identifiers is conditional on the CAG Section 251 approval. The data will be retained for the duration of the audit. The current audit contract with HQIP as the commission body and data controller is due to run until 31	Ensures regular review if there are any changes to IG permissions or project methodology.	NA	Epilepsy12 Project Team / RCPCH DPO

					March 2025 (Round 4).			
Being able to rectify or delete the data if requested.	2	2	4	**Eliminated**	Participating Health Boards and Trusts can edit and update their own local data on the data platform using their secure login and password protected access. Complete records will automatically be submitted once the specified submission deadline has passed and cannot be edited further. This allows the Epilepsy12 project team to conduct the annual analyses and reporting within the timeframes specified in the HQIP contract.	The RCPCH Subject Access Request procedure and Data Protection Policy will indicate that, for rights requests where the RCPCH is not the data controller, the request will be forwarded to the data controller which, in the case of Epilepsy12, is HQIP. Epilepsy12 Project Team members will adhere to a guide which sets out the process of dealing with subject access requests relating to project data.	In place, (reviewed March 2022)	Epilepsy12 Project Team / RCPCH DPO/ HQIP
Being able to update data regularly	1	2	2	**Accepted**	Participating Health Boards and Trust can edit and update their own local data on the data platform using their secure	Health Board or Trust Epilepsy12 Designated Leads monitor and control the data that is entered into		Epilepsy12 Project Team / RCPCH DPO

					login and password protected access. System validation and real-time feedback on the platform provides quality assurance and minimises data entry errors. Additional Data quality and validation checks are carried out on the data prior to analysis for the national report.	the audit platform and ensure via data quality checking functions that they are up to date with audit timelines and submission deadlines.		
Being able to restrict processing of the data if requested.	2	2	4	**Eliminated**	If a patient or parent asks us to restrict the processing of their data we will ensure we don't process or store the information on the data platform.	Ensure that audit staff know how to deal with rights requests.	In place	Epilepsy12 Project Team / RCPCH DPO
Individuals not adequately informed about their rights and how their data will be used	3	2	6	**Eliminated**	The privacy notice/patient information leaflet which includes the information outlined in Article 14 of GDPR. The DPO and CYP team will review the notice to ensure it meets GDPR requirements but is also age appropriate (aimed at	By providing individuals with information about how their data will be processed and targeting it towards the audience, this will ensure individuals are fully informed about their	In place Last updated January 2023.	Epilepsy 12 project team /RCPCH DPO

					children aged 13 and above). This will be updated and re-shared before any changes to the way data is collected are made	rights and how their data will be used and are clear about their choice to opt out.		

Corporate risks & compliance risks section- scoring and actions reviewed and updated on a quarterly basis on the main risk register. The score will be updated here as part of the annual review.								
What are the potential risks to the individuals whose personal data you hold?	**Probability of this happening** 1 Rare 2 Unlikely 3 Possible 4 Highly Likely 5 Almost certain	**Impact** 1 - minor 2- Moderate 3- Serious 4- Significant 5- Catastrophic	**Overall risk score** (PROBABILITY x IMPACT) + IMPACT	**Will risk be accepted, reduced or eliminated?**	**Current Mitigations**	**Actions Required**	**Expected completion date**	**Responsible owner**
IG not considered at the start of a new processing activity/system or procurement process- there is no data protection 'design by default'	**2**	**3**	**9**	**accepted**	**1. All staff aware of the PIA process and it is undertaken where there is a legal requirement.** **2. IG staff consulted on any**	**Information Governance Team: ELN briefing on PIA process to share with teams, regular College Huddle/Hub reminders. This will be following DPIA process**	**Ongoing review by Data Protection Committee**	**Data Protection Committee**

						new systems that manage data. **3. AUP Policy in place covering use of college systems and adhered to.** **4. Children's code working group in place and compliance overseen by DPC.** **5. Where staff will be undertaking a personal data transfer outside of the UK/countries with an adequacy decision, the transfer assessment form is completed on Topdesk and assessed by IG.** **6. Safeguarding mechanisms are put in place (e.g. Internati**	**review which is planned for 25/26 operational year.** **Information Governance Team: Regular College Huddle/Hub reminders, include in new induction policy** **Information Governance Team: ELN briefing on process to share with teams, regular College Huddle/Hub reminders** **Information Governance Team: ELN briefing on process to share with teams, regular College Huddle/Hub reminders, staff to support asset register review in a timely way. IG team setting up an annual ROPA/Retention Schedule review** **AUP currently being reviewed by IG and will be updated**		

					onal Transfer Agreements). 7. IG will do an annual review of the information asset register and review if there is a change in adequacy decision to identify affected processes 8. Digital involved in the procurement of any new IT systems. 9. AUP Policy in place covering college systems adhered to. 10. Agreement to not process identifiable data whether that is from adults or CYP autonomously including AI	following outcome of working group looking at the workflow for college devices and laptops for non-staff Digital / Information Governance Teams: Work with IG function to ensure relevant processes and staff guidance are appropriately updated on an ongoing basis as new programmes, processes or legalisation changes		
Inadequate IG Resourcing in place to meet minimal Legal Requirements:	**1**	**3**	**6**	**accepted**	**1. Staffing in place to adequately cover**	**1. DPO, SIRO and spec**	**Feb 2024**	**Data Protection Committee**

					compliance work. **2. IG budgets proportionate to IG requirements** **3. Data Protection Officer Appointed.** **4. Specialist training and development provided to IG staff as required.** **5. Potential new data protecitoon legislative bill coming into force later next year**	**ialist roles (e.g. cyber security) to continue to keep up to date with training and record on PDRs. Training Needs Analysis undertaken to identify specialist roles, training will be developed and also a skill audit will be circulated within first**	**Ongoing** **Ongoing**	

						6 months of 2025 to ascertain level of knowledge of staff (which includes specialist roles). 2. DPO to assess what the changes are once the Bill is confirmed and attending training/ update sessions to stay abreast of the changes.		
Third parties processing personal data without due diligence checks and	**3**	**3**	**12**	**accepted**	**1. Centralised procurement**	**Regular contract reviews**	**Ongoing review by**	**Data Protection**

legally required accountability mechanisms					**process that includes required IG checks/due diligence and includes informing digital where systems are involved.** **2. Article 28 contractual clauses in place with all data processors. DSAs in place where there is a DC-to-DC relationship.** **3. A processor can have many sub-processors so there needs to be a level at which due diligence is proportionate and a level of trust/risk acceptance.** **4.**	**(annual if data is high risk?)** **- Ensure contracts successfully migrated into new Contract Management Platform.** **- Ensure major changes to legislation, technology or best practice trigger relevant review(s) with suppliers.** **Regular contract reviews (annual if data is high risk?)** **- Ensure contracts successfully migrated into new Contract Management Platform.** **- Ensure major changes to legislation, technology or best practice trigger relevant review(s) with suppliers.**	**Data Protection Committee**	**Committee**
IG training awareness and culture: There is a lack of staff	**2**	**3**	**9**	**redced**	**1.** **2. Mandatory Data**	**To undertake audit to establish**	**Ongoing revie**	**Data Protection**

awareness in relation to information governance and staff are not trained on their responsibilities.					**Protection Training for all staff.** **3. Regular awareness campaign run by IG e.g. hub articles, town hall briefings, specialised training.** **4. Running regular phishing simulations.** **5. Running regular clear out days.** **6. Current training offered unlikely to meet requirements consistently. Need to identify and assess need, roles.** **7. Ensuring privacy notices are in place and easily accessible to data subjects** **8. Publishing and**	**current position all staff training - 95% completion of Data Protection eLearning.** **Immediate consideration to develop literature to disemmante on mass identify what constitutes handling of data and how this should be managed in line with role** **Privacy notices in situ and reviewed and republished in line with line with legisation changes. To continue to update on The Hub, Huddles etc. Fixing the cookie website issue. IG undertaking a major overhaul of privacy notices and will be creating a privacy hub.** **Privacy notices in situ and reviewed and republished in line with line with legisation changes. To continue to**	**w by Data Protection Committee**	**Committee**

					regularly reviewing IG Policies, Procedures and Guidance. 9. Regular reporting to SLT, AFRC and DPC.	update on The Hub, Huddles etc. Reporting matrix /AOB to be identified with submission dates established so this work can be scheduled as required. Process to be established to identify any information that may be at risk, then to establish who will undertake audit. Once Record of Processing Activity (ROPA) is restructured and finalised we can spot check processing activities to assess compliance and accuracy against the ROPA. Not to be scored currently as process not in place. Fixing issue with dotdigital relating to old campaign lists.		

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		
Name of DPO		
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)		
Does the DPIA explain how each individual's rights are Managed? See section on individuals rights		
Are safeguards in place surrounding international transfer? See section on sending information outside the EEA		
Was consultation of the document carried out and with whom?		
Organisations ICO registration number		
Organisations ICO registration expiry date		
Version number of the DPIA you are submitting		
Date completed		

Appendix 2 Guidance for completing the table

What are the potential risks to the individuals whose personal data you hold?	See examples above

Likelihood of this happening (H,M,L)

Likelihood score	Description	Example
1	Very unlikely	May only occur in exceptional circumstances
2	Unlikely	Could occur at some time but unlikely
3	Possible	May occur at some time
4	Likely	Will probably occur / re-occur at some point
5	Very likely	Almost certain to occur / re-occur

Impact (H,M,L)

Impact scores	Description	Example
1	Insignificant	No financial loss; disruption to day to day work manageable within existing systems, no personal data loss/ no breach of confidentiality
2	Minor	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
3	Moderate	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
4	Major	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
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?