NHS
Herts Valleys
Clinical Commissioning Group

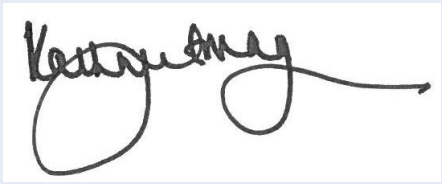
Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
Title of Document		Data Protection Impact Assessment Policy (Privacy by Design)
Could this policy be incorporated within an existing policy?		no
Does this policy follow the style and format of the agreed template?		yes
Has the front sheet been completed?		
Is there an appropriate review date?		yes
Does the contents page reflect the body of the document?		yes
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?		yes
Are all appendices appropriate and/or applicable?		yes
Have all appropriate stakeholders been consulted?		yes
Has an Equality Impact Assessment been undertaken?		yes
Is there a clear plan for implementation?		yes
Has the document control sheet been completed?		yes
Are key references cited and supporting documents referenced?		yes
Does the document identify which Committee/Group will approve it?		yes

Plans for communicating policy to – staff; practice membership; public (as appropriate)		Via the weekly staff news bulletin

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Chief Finance Officer	Date	12/6/18
Signature			

Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Chief Executive	Date	12/6/18
Signature			

NHS
Herts Valleys
Clinical Commissioning Group

Data Protection Impact Assessment Policy (Privacy by Design)

Version Number	V.2
Ratified By	Virtual IG Group Executive Team
Date Ratified	**June 2018**
Name of Originator/Author	Information Governance Manager
Responsible Director	Caroline Hall
Staff Audience	All Staff
Date Issued	July 2018
Next Review Date	June 2019

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
V1		New Document	May 2016	Ruth Boughton/Rob Lindop
V2		Annual Review, Add DPO role Add GDPR requirements	May 2018	IG Manager

CONTENTS

1. INTRODUCTION

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks to a project.

You must complete a DPIA at the start of a new project that involves or may involve the processing of personal data.

Please see Appendix One to help decide whether to carry out a DPIA

It is also good practice to carry out a DPIA for any other major project which requires the processing of personal data.

If the CCG has a reportable data breach the Information Commissioners Office (ICO) will ask the CCG whether they have carried out a DPIA. It is often the most effective way to demonstrate to the ICO how personal data complies with the DPA 2018/GDPR.

2. PURPOSE

The aim of the policy is to make sure that HVCCG has considered all aspects of Information Governance before beginning any new type of processing which is likely to result in high risk.

The ICO says you **must** complete as DPIA if you plan to use systematic and extensive profiling, process special category or criminal data on a large scale, use new technologies, use profiling or special category data to decide on access to services.

A DPIA must:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks.

To assess the level of risk, you must consider both the likelihood and the severity of any impact to individuals data. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

You must consult with the Information Governance Manager and the Data Protection Officer (DPO) and where relevant individual experts, if a high risk is identified which cannot be mitigated, the DPO will consult with the Information Commissioner (ICO) before processing can begin.

The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to process the data, or ban the processing altogether.

Please refer to Appendix B C and D for the DPIA process map and template.

3. DEFINITIONS (as per GDPR)

Data Protection Impact Assessment (DPIA)
A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

Personal Data
Any information relating to an identified or identifiable natural person (data subject) who can be identified directly or indirectly by reference to any identifier such as a name, address, or online identifier such as an IP address.

When processing Personal Data, the CCG must ensure that it identifies a legal basis for processing under Article 6 of GDPR

Special Categories of Personal Data (previously known as sensitive data under the DPA 1998).

When processing data that is classed as Special Categories of personal data, the CCQ must ensure that it identifies a legal basis for processing under Article 9 as well as Article 6 of GDPR.

Special Categories of data consists of Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, membership to trade unions, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning physical or mental health condition, data concerning a natural persons sexual life or sexual orientation.

Criminal offences committed or alleged offences and any conviction is now processed under the Data Protection Act 2018 Section 29 (data protection bill)

Pseudonymised data
Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional

information, provided that such additional information is kept separately i.e. Data in which individuals are distinguished through the use of a unique identifier.

Profiling

Any forms of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning individuals performance at work, economic situation, health, personal preferences, interests, reliability, behaviour and location or movement.

Data Sharing Contracts (DSC) and Data Sharing Agreements (DSA)
The Data Sharing Contract (DSC) is an overarching document that contains the principles to be adhered to in data sharing and legal requirements whilst the Data Sharing Agreement (DSA) necessarily covers the specifics of the data that is being shared, for which purpose, how it will be transferred, stored etc.

4. ROLES AND RESPONSIBILITIES

All information used within the NHS is subject to handling by different departments and individuals. At no time should the confidentiality of this information ever be compromised.

Therefore in order to safeguard all information adequately, at all times, it is vitally important that all individuals are clear about their responsibilities in relation to this information. In order to ensure clarity amongst all concerned, the CCG, will fully promote and support the mandatory completion of Information Governance Training.

4.1 Roles and Responsibilities within the Organisation

Chief Executive
The Chief Executive of the CCG and has overall accountability and responsibility for Information Governance in the CCG and is required to provide assurance, through the Statement of Internal Control that all risks to the CCG, including those relating to information, are effectively managed and mitigated.

Senior Information Risk Owner (SIRO)
Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embed information risk management into the overall risk management culture of the CCG.

The SIRO, DPO and Caldicott Guardian will receive via the IG Virtual Group all privacy impact assessments and or sharing agreements for approval, Approval is then reported via the SIRO report to both the Senior Leaders Team and the Executive Team.

Information Asset Owners
The Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets for the organisation. It is a core IG objective that all Information Assets of the organisation are identified and that the business importance of those assets is established.

The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IOA will therefore document, understand and monitor.

- What information assets are held, and for what purposes
- How information is created, amended or added to over time
- Who has access to the information and why

Project Lead
The project lead will have been given authority and responsibility to manage the project on a day to day basis and deliver the required outcomes within constraints agreed by the board.

Caldicott Guardian
The Caldicott Guardian plays a key role in ensuring Herts Valleys CCG satisfies the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of the organisation, the Caldicott Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information.

The Caldicott Guardian also has a strategic role, which involves representing and championing privacy and information sharing requirements at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework.

Data Protection Officer and Information Governance Manager
The Data Protection Officer, supported by the Information Governance Manager are responsible for ensuring effective management, accountability, compliance and assurance for all aspects of IG for the CCG. They will offer advice and assistance to staff who need to complete a Data Protection Impact assessment or develop a data sharing agreement.

Virtual Information Governance Group
The Virtual IG Group are responsible for approving DPIA's that are presented to the group from the project manager via the Information Governance

Manager, any DPIA that requires financial approval will also be approved by the Executive Team.

Managers and Staff
Staff will only use the minimum personal data to satisfy a legal purpose.

Individual members of staff are accountable for:

- The content of the record (e.g. staff file, complaints file)
- Ensuring records and information meet the standards required by the CCG.
- Ensuring they access training with regards to information governance and keeping information safe and secure.

4.2 Consultation and Communication with Stakeholders

The following groups have been consulted:

- Virtual IG Group
- Senior Leadership Team
- Executive Team.

5. CONTENT

Introducing a new process or system.
Information Governance staff must be involved at the earliest possible stage to advise on potential issues arising from introducing a new system or process and ensure that the appropriate information governance clauses appear in any subsequent contract or service level agreement in the first instance.

When introducing a new process or system, an assessment must be carried out to establish the following: (please refer to Appendix D)

- The objectives of the new system/process
- The requirements /benefits
- The justification for a new system/process
- Whether the requirements are achievable using existing systems
- The minimum hardware requirements needed to rum the system e.g. network, infrastructure, servers, PC's software compatibility.
- Will the new system link to any existing systems/processes?
- Resource needed to successfully implement the system
- Support and maintenance required
- How many staff will use the system?
- What are the training implications?
- What is the cost?
- What are the estimated capital costs and on-going revenue costs?
- Will the project comply with privacy laws and regulations?
- Is a Data Protection Impact assessment required?
- What legal basis will be used for processing the data?

- Will there be a risk to confidential information?
- Will there be a risk to corporate information?

Refer to Appendix B Data Protection Impact Assessment Flow Diagram

What is an Information Governance Data Protection Impact Assessment (DPIA)

A DPIA is a way to systematically and comprehensively analyse processing and help identify and minimise data protection risks.

DPIAs should consider compliance risks as well as broader risks to the rights and freedoms of individuals. The focus is on the potential for harm.

A DPIA does not have to eradicate the risk altogether, but should help to minimise risks and assess whether the remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance.

A DPIA is not a one off exercise and should be seen as an ongoing process, which is regularly reviewed.

The DPIA should be completed at the project design/system release planning stage to make sure that potential risks are identified early and solutions can be developed to mitigate any risks before the new process, system is implemented.

Why should I complete a DPIA?

- To identify privacy risks to individuals/organisations
- To identify whether a sharing agreement is required.
- To identify privacy and data protection compliance liabilities for the CCG.
- To install public trust and confidence in the project
- To avoid expensive, inadequate “bolt-on” solutions
- To inform your communications strategy

When should I start a DPIA?

DPIAs are most effective when they are started at an early stage of a project, when:

- The project is being designed
- You know what you want to do
- You know how you want to do it

- You know who else is involved
- Before decisions are set in stone
- Before you have procured systems
- Before you have signed contracts/agreements.

Responsibility for Completing the DPIA

The Information Asset Owner (IAO)/Project Lead is responsible for completing the DPIA for a new system implementation/release/process. IAO's understand and address risks to the information assets they own, they provide assurance to the Senior Information Risk Owner (SIRO) on the security and use of these assets.

Consultation, Approval and Ratification Process for the DPIA

The DPIA must be approved by the IG Virtual along with the SIRO before final executive approval (if required), any concerns or issues will be escalated to the SIRO.

Data processing activity must comply with the GDPR/Data Protection Act 2018 (DPA) and section 251. A DPIA is a process which helps access privacy risks to the organisation and individuals in the collection, use and disclosure of information.

The form Appendix D must be used for both internal and partnership projects that require the collection and or use of personal information.

When final approval has been gained by the IG Virtual group, the approval evidence will be stored in the Information Governance shared drive.

Sharing Protocols

Where a new process involves routinely sharing patient confidential data with another organisation a sharing protocol will need to be in place to establish:

- What information will be shared
- Who will have access to it
- How access will be granted
- The legal basis on sharing the data (the Data Protection Principles must be fully considered)
- Who is responsible for the annual review.

A signed copy of the sharing agreement by the Caldicott Guardian must be sent to the Information Governance Manager.

Contracts

Each individual identified in the process outlined in this policy will ensure that all contracts and service level agreements have the appropriate Information Governance and Data Protection clauses.

It is really important that these processes are completed before:

- Decisions are set in stone
- You have procured systems
- You have signed contracts/Memorandums of Understanding/agreements.

6. MONITORING COMPLIANCE

Monitoring will be undertaken by Information Governance Manager, who will provide regular reports to the Senior Leadership Team and the SIRO.

7. EDUCATION AND TRAINING

Mandatory Information Governance Training

8. REFERENCES

GDPR/Data Protection Act 2018
Data Protection and Security Toolkit.
Human Rights Act
Freedom of Information Act 2000
Environmental Regulations Act 2005
Access to Health Records Act 1990 (Where not superseded by the Data Protection Act 1998)
Computer Misuse Act 1990
Copyright, designs and patents Act 1988 (as amended by the Copyright Computer Programs Regulations 1992)
Crime and Disorder Act
Electronic Communications act 2000
Regulations of Investigatory Powers Act 2000
ICO Data Sharing Code of Practice

9. ASSOCIATED DOCUMENTATION

HVCCG Information Governance Management Framework
HVCCG Information Governance Strategy
HVCCG Information Governance A Guide for all Staff
HVCCG FOI Policy
HVCCG Information Lifecycle Management Policy
HVCCG Mobile Devices Policy
HVCCG DPA & Confidentiality Policy
HVCCG Email and Internet Policy
HVCCG Information Risk Policy

HVCCG Information Security Policy
HVCCG Safe Haven Policy
HVCCG Sharing Policy
HVCCG Registration Authority Policy
HVCCG Fair Processing Notice

APPENDIX A:

Equality Analysis - Equality Impact Assessment Screening Form

Very occasionally it will be clear that some proposals will not impact on the protected equality groups and health inequalities groups.

Where you can show that there is no impact, positive or negative, on any of the groups please complete this form and include it with any reports/papers used to make a decision on the proposal.

Name of policy / service	HVCCG Data Protection Impact Assessment Policy
What is it that is being proposed?	The CCG Data Protection Impact Assessment aims to detail how the CCG will meet its legal obligations and NHS requirements concerning privacy by design. The requirements within the Policy are primarily based upon the GDPR, which is the key piece of legislation covering privacy impact assessments..
What are the intended outcome(s) of the proposal	That all CCG staff are aware of their responsibilities and are aware of legal requirements and CCG processes.
Explain why you think a full Equality Impact Assessment is not needed	This policy sets the information governance requirements in relation to Data Protection Impact Assessments.
On what evidence/information have you based your decision?	The policy refers to GDPR regulations
How will you monitor the impact of policy	Via the Data Protection and Security Toolkit

or service?	
How will you report your findings?	To the Senior Leadership Team via toolkit action plans and compliance reports

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact Assessment is not required.	
Assessors Name and Job title Date May 2018	Ruth Boughton Information Governance Manager

APPENDIX B

Process for Data Protection Impact Assessments

New Project → Identify a need for DPIA → Complete a DPIA → IG Team Review → Approval by SIRO (via IG Sub Group

Example of project:	Project lead to:	Project lead to:	Send to IG Team	IG Sub Group/Executive Team:
New IT system Data sharing initiative Legislation, policy or strategies which will impact on privacy through the collection of information.	Identify if the project involves the use of personal data, or have an impact on the privacy of individuals.	Describe information flows Identify privacy risks Identify and evaluate privacy solutions Consult with internal and external stakeholders as needed	To review DPIA and ask for further information should it be required. To log DPIA number and data send for ratification.	To formally approve or ask for further information. To notify the project lead that the DPIA has been approved. DPIA log to be updated

Appendix C

DPIA screening checklist

You must always carry out a DPIA if you plan to:

- Carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
- Process special category data or criminal offence data on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

You consider carrying out a DPIA if you plan to carry out any other:

- Evaluation or scoring.
- Automated decision-making with significant effects.
- Systematic
- Processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.
- Consider carrying out a DPIA in any major project involving the use of personal data.
- **If you decide not to carry out a DPIA, you must document your reasons.**

DPIA process checklist

- Describe the nature, scope, context and purposes of the processing.
- ask our data processors to help us understand and document their processing activities and identify any associated risks.
- consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- ask for the advice of our data protection officer.
- check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure data protection compliance.
- do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
- identify measures we can put in place to eliminate or reduce high risks.

- record the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- implement the measures identified, and integrate them into our project plan.
- consult the ICO before processing if we cannot mitigate high risks.
- keep our DPIAs under review and revisit them if necessary.

The CCG is required to complete a DPIA before we begin any type of processing which is "likely to result in high risk" .All new IT systems, databases or on-line data submission systems introduced to the CCG containing person identifiable data (PID), whether patient or staff, must be approved by the IG SUB Group to ensure they comply with current technical and information governance requirements. This checklist is to be used by the Information Governance Manager to ensure compliance with the General Data Protection Regulations of new processes, software and hardware involving the processing of person identifiable data (PID). All processes, electronic or manual, software or hardware incorporating the processing of PID must be tested for GDPR/confidentiality compliance prior to implementation/commencement and approved by the IG Sub Group. The Information Governance Manager will periodically carry out data protection compliance checks on existing processes and a report will be made to the appropriate Director and the Senior Leadership Team detailing findings and recommendations if compliance is not met.

Please complete this form as part of your project initiation documentation and submit to the Information Governance Manager Ruth Boughton for approval.

Details/Consideration	Notes	Complete All Boxes
System/new(revised) process name	What is the system commonly known as?	
Who is the Supplier?	Give full contact details including address, telephone number and name of person responsible for support.	
Which department is introducing the new system/database/process?	Please state system sponsor.	
When is it anticipated the system will be implemented? Will the system integrate with any other Trust systems?	State anticipated 'go-live' date. Give brief outline of testing procedures, if applicable. State whether the system will pull information such as demographics from any other system in use at the Trust.	
Is personal data being processed? Can we legitimise processing of	The General Data Protection Regulations defines personal data as any information held in any format that can identify a living individual. However a duty	If yes - legitimate process (Please tick – at least one of the conditions below MUST apply)

<table>
<tr><th>Details/Consideration</th><th>Notes</th><th colspan="6">Complete All Boxes</th></tr>
<tr><td rowspan="2">personal data in accordance with the terms of Article 6 of the GDPR? (Appendix 1)</td><td rowspan="2">of confidentiality still applies to the deceased so this form should still be completed for systems/processes involving the use of personal data of the deceased.</td><td>Consent (a)</td><td></td><td>Contract (b)</td><td></td><td>Legal Obligation (c)</td><td></td></tr>
<tr><td>Vital Interests (d)</td><td></td><td>Public interest (e)</td><td></td><td>Legitimate interest (f)</td><td></td></tr>
<tr><td rowspan="5">Is sensitive (special) personal data being processed?

Can we legitimise processing of sensitive personal data in accordance with the terms of Article 9 of the GDPR (Appendix 2)</td><td rowspan="5">Sensitive personal data is personal data relating to a person’s race, political beliefs, trade union membership, sexual orientation, health, biometrics (where used for ID purposes),genetics, ethnic origin, religious beliefs.</td><td colspan="6">If yes – legitimate process, article 6 and 9 conditions need to be satisfied (Please tick all that apply)</td></tr>
<tr><td>Explicit consent (a)</td><td></td><td>Employment (b)</td><td></td><td>Vital Interests (c)</td><td></td></tr>
<tr><td>Legitimate activates (d)</td><td></td><td>Made public by DS (e)</td><td></td><td>Legal Claim (f)</td><td></td></tr>
<tr><td>Public interest (g)</td><td></td><td>Health & Social Care (h)</td><td></td><td>Public Health (i)</td><td></td></tr>
<tr><td>Research (j)</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Is the system capable of capturing and storing the NHS number?</td><td>This is now a requirement of all new systems. Steps must be taken to ensure the NHS number is captured and stored.

If the answer is yes, how is the NHS number verified?

If the answer is no, what steps are being taken to ensure this requirement is met?</td><td colspan="6"></td></tr>
<tr><td>Does the system have a reporting facility?

Is the system able to produce a printout of all personal data to satisfy the subject access provision of the General Data Protection</td><td>Briefly summarise the standard reporting facility of the system.

The system should have the facility to produce a printout of all personal data held.</td><td colspan="6"></td></tr>
</table>

Details/Consideration	Notes	Complete All Boxes
Regulations		
Briefly describe the purpose, nature and context of the processing Who is the Information Asset Owner? (The person responsible for the process/system?) What steps have been taken to ensure the data processor complies with data protection? How have you assessed the system security measures? Is there an ongoing procedure in place to monitor compliance with these measures?	The word 'system' is used to mean new software/hardware. An internal named lead must be the system owner and be responsible for the system management. If maintenance/support is an external company is there a robust contract is place including security of information transferred and external staff accessing data, etc? Have you identified any associated risks to the information?	
Will the data be used for the purpose of direct care?		
Will the data be used for HR/staff records?		
If consent is identified as the reason to legitimise processing what happens when consent is withdrawn? Are individuals offered the opportunity to restrict processing of their personal data?	Describe the process and what will happen to the data if consent is withdrawn. If consent is withdrawn can vital interests/legitimate interest still be cited for continuing use of the system?	

Details/Consideration	Notes	Complete All Boxes
If so when is that opportunity offered? Are procedures in place for maintaining an up to date record of use of personal data. If so how often and by whom?		
Data set/programme supported.	If this is a nationally recognised data set, programme or initiative please give title or outline description	
Who is the Information Asset Administrator who will be responsible for the data quality (accuracy) of the information in the process/system? How will the data be checked for relevancy, accuracy and validity? How often will the data be checked and validated?	An internal member of staff must be named as the responsible person for maintaining the system/database and who will carry out data validation checks. Work place procedures must be provided and appended to this application. List of relevant procedures.	
Who will have access to the system and how will that access be controlled? Will training on use of the system be provided and a list of trained personnel maintained? Is there a process in place to ensure all users have attended Trust mandatory data protection training?	Give description of potential users and authorisation process. Include process used when users leave employment and how the account will be disabled. Evidence mandatory training. Maintain list of users trained on the system.	

Details/Consideration	Notes	Complete All Boxes
Is identifiable data shared with other organisations via the system?		
If yes, please give brief details If the PID is to be transmitted electronically does the method of transfer comply with data encryption/removable media policies?	For example, the system collects clinical data that is used by another CCG/Hospital when the patient is in contact with them. (Please list organisations data will be shared with). Detail how will the data be moved. (I.e. on line, encrypted media, hard copies, etc.)	
Is anonymised or aggregate data shared with other organisations?	For example for national or local audit or benchmarking. If yes give brief description and organisations who will receive the data	
What will happen to the personal data when it is no longer required? Who will take responsibility for ensure disposal of data in accordance with National and local retention and disposal policy timescales?	E.g. Data will be archived and subsequently destroyed securely. Workplace procedure will need to be in place outlining the process.	
Does the process/system have an adequate level of security to ensure that PID is protected from unlawful or unauthorised access and from accidental loss, destruction or damage?	Confirmation of security and backup arrangements required.	
Does the process/system enable timely location and retrieval of personal data to meet Subject Access requests?	Describe retrieval process. If the process refers to another paper or electronic system then this process is also required, e.g. tracing of paper case notes by an electronic system.	
Is PID being sent outside the UK?	If yes seek further guidance from the Information Governance Manager	
Is the purpose of processing the	*IG Team to advise. The IG Team will ensure that the*	

Details/Consideration	Notes	Complete All Boxes
personal data listed in the Trust's Notification to the Information Commissioner?	*purpose for processing is listed in the current Notification and Fair Processing Notice.*	

Approval for new system granted YES/NO
If no, reason for refusal:

Signed _____ Print Name _____

Position: On behalf of the IG Committee
_____

_____

Date
_____

ARTICLE 6 OF THE GDPR

At least one of the following conditions must be satisfied to legitimise processing of personal data:

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

ARTICLE 9 OF THE GENERAL DATA PROTECTION REGULATIONS

At least one of the following conditions must be satisfied to legitimise processing of sensitive personal data:

The conditions are listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(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;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Some of these conditions make reference to UK law, and the GDPR also gives member states the scope to add more conditions. The Data Protection Bill includes proposals for additional conditions and safeguards, and we will publish more detailed guidance here once these provisions are finalised.