Bolton Clinical Commissioning Group

Data Protection Impact Assessment Procedure and Proforma

Policy Number	**IG011**
Target Audience	**CCG Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**28th May 2020**
Last Review Date	**April 2020**
Next Review Date	**28th May 2022**
Policy Author	**IG Team**
Version Number	**V5.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	September 2013	M Robinson D Sankey	Progress to CCG Executive for approval
1	September 2013	CCG Exec	Approved
1.1	July 2015	IG Team	Organisation change to GMSS and rebranding of PIA to BCCG
1.2	July 2016	IG Team	No substantial changes. Review for Approval
2.0	August 2015	IM&T Operations Board	Approved
3.0	April 2018	IG Team	Reviewed in line with GDPR
4.0	May 2018	IM&T Operations Board	Approved
5.0	May 2018	CCG Chief Officer	Approved
5.1	April 2020	IG Team	Reviewed and updated in line with ICO guidance

Analysis of Effect completed:	By: M Robinson	Date: September 2013

What are Data Protection Impact Assessments (DPIAs)?

Article 35(1) of the General Data Protection Regulations (GDPR) says that you must complete a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of individuals:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

Failure to adhere to this Article and complete a DPIA may result in action by the Information Commissioner's Office (ICO).

DPIAs help organisations identify, assess and mitigate or minimise privacy risks with data processing activities, where *personal data* is being processed.

A DPIA is a risk assessment which asks questions about a process or new system based on data protection / data quality / information security and technology.

When should you complete a Data Protection Impact Assessment?

If you are doing any of the following:

- setting up a new process using personal data
- changing an existing process which changes the way personal data is used
- procuring a new information system which holds personal data

A DPIA must be completed as early as possible to ensure risks can be identified and mitigated to an acceptable level.

If the data is to be **anonymised prior** to any processing you may not need to complete this DPIA, to check, review and complete Section 2.

Who needs to complete a Data Protection Impact Assessment (DPIA)?

It is the Information Asset Owners responsibility to ensure this is completed and submitted. They can delegate this task to an Information Asset Manager (IAM) or Administrator (IAA) / Project Manager(s) and or suppliers of a system / asset.

Next steps

1. Please complete each section with as much detail as possible. Your IG team will be able to assist you with Section 4 but may need additional information from you. Note that you may need input from other parties (i.e. IT, other service departments, suppliers etc)/
2. Once you submit the DPIA for approval to your IG Team:
    a. The DPIA proforma will be vetted and you may receive some comments / questions asking for further information. Please answer these promptly and resend the DPIA.
    b. If the DPIA is considered to be a 'high risk' by the IG Team they will need to consult with the CCG's Data Protection Officer (DPO) and ICO and await their response.
    c. The DPIA if low or medium risk will be presented for approval at the IG Board, where the DPO is in attendance and key subject matter experts.
3. Once approved, the process / system can start to be introduced or modification to an existing system / process can continue.
4. ***If you proceed with the initiative without completing a DPIA and without approval via the IG DPIA approval process, you will be putting the CCG at risk of being in breach of the Data Protection legislation (GDPR) which may result in disciplinary procedures being invoked by the ICO***.

For a complete DPIA Process Flowchart please refer to the Appendix.

Section1: Basic Information

Reference:
DPIA Title:

DPIA Contact Details : *(please list all parties involved in this DPIA, note this can be Project Managers / IAOs / IAAs or whoever has been requested to complete the proforma):*

Name	Role	Organisation / Department	Email	Tel. No

Key Roles: Data Controller (s) / Data Processor (s) / System Supplier (s)

Accountability Description	Organisation and Department	Contact Details (include DPO)	Comments
Data Controller(s) – who determines the way data is processed? If Joint Data Controllers please list all parties involved			
Data Processor(s) – is data being processed on behalf of Data Controller(s) (please note this is not the system supplier)			
System Supplier(s) – IT systems that hold and process data under direction by			

	the Data Controllers / Data Processors			
New Initiative / System / Process Name:				
Date Initiative due to go live:				
Description, purpose of and reason for the initiative *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*	**Description, purpose and benefits (provide as much detail as possible):** **Types of data being collected (please refer to Appendix for definition):** ☐ Personal Data ☐ Special Category Data **Who is the Data Subject (i.e. patient, staff etc.):** **How will the data be collected:** **How will the data be used:**			

	Can the data be anonymised / pseudonymised? Does the Personal Data need to remain identifiable: **How often will you be collecting and using the Personal Data? i.e. daily, one off:** **Will the Personal Data be disclosed outside of the parties to this initiative (listed above in Key Roles section) in identifiable form and if so to who, how and why:** ☐ **Yes – provide details below No** ☐ **Specify the demographic / cohort / criteria** e.g. all adults over the age of 65 and **Specify the borough(s) or GM wide:** **How long do you expect this initiative to last:** ☐ End of contract period ☐ Specific time period – specify? ☐ Lifetime of system (where the initiative or project relates to a new or revised ICT system) ☐ Other – specify …….. **What is the nature of your relationship with the individual data subjects for this initiative? *This enables IG to ascertain the lawful basis for processing***

<table>
<tr><td></td><td>Provision of health/social care ☐ | Protecting the health of the general public ☐ |
Local audit to assure safe health and social care ☐ | Checking quality of care, beyond local audit ☐ |
Supporting research ☐ | Staff employment ☐ | Other - specify:</td></tr>
<tr><td>Link to wider initiative (if applicable):</td><td></td></tr>
<tr><td>Is this initiative in line with or achieving national or local guidance/
strategy or mandate?</td><td>☐ Yes
☐ No
If yes, please provide details below:</td></tr>
<tr><td>Information Technology / System Supplier Involvement</td><td>List applicable information technology kit / systems / software for this initiative to take place (please list current and / or new):

<table>
<tr><th>System name / IT Kit</th><th>Used by e.g. organisation and dept.</th><th>Parties / System Supplier</th><th>Description of System / IT Kit</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="3">Confirmation of IT Involvement / IT Leads Support</th></tr>
<tr><th>Name:</th><th>Organisation:</th><th>Confirm (Yes / No) if aware / involved regarding this initiative. If No, please seek input prior to submitting this DPIA</th></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

Confirm all relevant organisations listed above have or are working towards Cyber Essentials	Organisation / Parties / System Supplier	Cyber Essentials Y / N or Working towards / cyber compliance defined under terms of contract

Section 2: Screening Questions

The screening questions below highlight key areas which have the potential to cause privacy risks. Answers to these questions will highlight any particular privacy risks / issues that can assist you to populate risk assessments.

Potential Privacy Risk		Yes	No	Unsure	Comments *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
a)	Will the new system / process / initiative rely on automated processing without human intervention to make a decision?	☐	☐	☐	
b)	Will the new system / process / initiative involve large scale processing* of special categories of data (such as health and genetic data)? *refer to Definitions in Appendix	☐	☐	☐	
c)	Will the processing involve systematic monitoring of a public area on a large scale (e.g. CCTV)?	☐	☐	☐	
d)	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?	☐	☐	☐	
e)	Will the initiative involve the collection of new information about individuals?	☐	☐	☐	

f)	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐	☐	☐	
g)	Will the initiative require you to contact individuals in ways which they may find intrusive?	☐	☐	☐	
h)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐	☐	☐	
i)	Will the initiative involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition	☐	☐	☐	
j)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐	☐	☐	
k)	Will the initiative compel individuals to provide information about themselves?	☐	☐	☐	

If you answered **YES or UNSURE** to any of the above you need to continue with the Data Protection Impact Assessment.

***Sign off if no requirement to continue with Data Protection Impact Assessment*:**	
Confirmation that the responses to a – h above is NO and therefore there is no requirement to continue with the Data Protection Impact Assessment	
Agreed by:	Click here to enter name of group or individual(s).

Section 3: Data Items

Tick the boxes regarding the data items that will be processed for this initiative, system, project:

Personal Details
Information that identifies the individual and their personal characteristics

- ☐ Forename(s)
- ☐ Surname
- ☐ Address
- ☐ Postcode
- ☐ Date of Birth
- ☐ Age
- ☐ Gender
- ☐ Physical Description
- ☐ Home Tel Number
- ☐ Mobile Tel Number
- ☐ Other Contact No.
- ☐ Email Address
- ☐ GP Details
- ☐ Legal Representative (Next of Kin)
- ☐ NHS Number
- ☐ NI Number
- ☐ Photographs/Pictures
- ☐ Other, list below:

Physical or Mental Health or condition

- ☐ Yes
- ☐ No
- ☐ N/A

List any data items below:

Sexual Identity and life

- ☐ Yes
- ☐ No
- ☐ N/A

List any data items below:

Trade Union Membership

- ☐ Yes
- ☐ No
- ☐ N/A

List any data items below:

Family lifestyle & social circumstances
Information relating to the family of the individual and their social circumstances

- ☐ Marital / partnership status
- ☐ Carer / relatives
- ☐ Children / Dependents
- ☐ Social status e.g. housing
- ☐ N/A

List other data items below:

Education & Training

- ☐ Education / Training
- ☐ Qualifications
- ☐ Professional Training
- ☐ N/A
- ☐ Other, please list below:

Employment Details

- ☐ Employment Status
- ☐ Career Details
- ☐ N/A
- ☐ Other

Financial Details

- ☐ Income
- ☐ Salary
- ☐ Benefits
- ☐ N/A
- ☐ Other, please list below:

Religious of other beliefs of a similar nature

- ☐ Yes
- ☐ No
- ☐ N/A

List any data items below:

You must confirm that the data items you have ticked above are relevant and necessary for this initiative and there is a justified reason for their use. Tick the box below to confirm this:
☐ **Confirm**

Offences including alleged offences
Information relating to any offences committed or alleged to have been committed by the individual

- ☐ Yes
- ☐ No
- ☐ N/A

List any data items below:

Criminal Proceedings, outcomes and sentences

- ☐ Yes
- ☐ No
- ☐ N/A

List any data items below:

Section 4: Legal Basis for Processing the Data

1. Is the data for the initiative / within the system going to be used for Direct Care?

The definition of direct care is: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes:-

- *supporting individuals' ability to function and improve their participation in life and society*
- *the assurance of safe and high quality care and treatment through local audit,*
- *the management of untoward or adverse incidents*
- *person satisfaction including measurement of outcomes*

undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care

☐ **Yes (go to Q2)** ☐ **No (go to Q3)**

DPIA Question	DPIA Response	Comments
2. Please confirm the legal basis for processing for Direct Care	I confirm that this initiative is for the provision of Direct Care and confirm the legal basis for processing under Article 6 and 9 of the GDPR and the Data Protection Act 2018 (Sch 1, Part 1) is as follows: ☐ **Art 6 (1)(e)'…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'** **And,** **DPA 2018 - Sch1,Part 1-Health or Social Care** ☐ **Art 9 (2)(h)'…medical diagnosis, the provision of health and social care or treatment or the management of health or social care systems…'** **And,** **DPA 2018 - Sch1,Part 1-Health or Social Care** In some cases, explicit consent can be obtained for processing for direct care, please state if you will be obtaining explicit consent for the processing for Direct Care at all? ☐ Yes explicit consent will be obtained for Direct Care as per GDPR Article 6 (1)(a) – Consent and Article 9 (2)(a) - Explicit Consent ☐ No	

<table>
<tr><th>DPIA Question</th><th>DPIA Response</th><th>Comments</th></tr>
<tr><td></td><td>In other cases, processing for Direct Care may also come under ‘vital interests’ of the individual , if so select:
☐ Article 6(1)(d) - Vital Interests
☐ Article 9(2)(c) - Vital Interests</td><td></td></tr>
<tr><td>3a. Is the data for the initiative / within the system going to be used to deliver indirect care?

3b. What is the legal basis that permits you to carry this out for indirect care?

3c. Please confirm the legal basis under Art 6 (for personal data) and 9 (for special categories of data) under GDPR for processing for this purpose</td><td>☐ Yes, please state below the indirect care reason and legal basis below (3c)
☐ No, please go to question 4

Indirect Care Processing
☐ Commissioning
☐ Monitoring Health and Social Care
☐ Public Health
☐ Research
☐ Other, please specify below

☐ Explicit Consent
☐ Section 251 of the NHS Act 2006
☐ The Health and Social Care Act 2015
☐ The Care Act 2014
☐ Other Legal Gateway, please state below:

<table>
<tr><th>Article 6 lawful basis for processing</th><th>Article 9 – lawful basis for processing special categories of data</th></tr>
<tr><td>☐ Article 6 (1)(a) - Consent</td><td>☐ Article 9(2)(a) - Explicit Consent</td></tr>
<tr><td>☐ Article 6 (1)(b) - Contractual Necessity</td><td>☐ Article 9(2)(b) - Employment</td></tr>
<tr><td>☐ Article 6(1)(c) - Compliance with legal obligations</td><td>☐ Article 9(2)(c) - Vital Interests</td></tr>
<tr><td>☐ Article 6(1)(d) - Vital Interests</td><td>☐ Article 9(2)(d) - Charity or not for profit bodies</td></tr>
<tr><td>☐ Article 6(1)(e) - Public interest or in exercise of official authority</td><td>☐ Article 9(2)(e) - Manifestly made public by data subject</td></tr>
<tr><td>☐Article 6(1)(f) - Legitimate Interests</td><td>☐ Article 9(2)(f) - Legal Claims</td></tr>
</table>
</td><td></td></tr>
</table>

DPIA Question	DPIA Response	Comments
	☐ Article 9(2)(g) - Substantial public interest ☐ Article 9(2)(h) - Health and Social Care ☐ Article 9(2)(i) - Public Health ☐ Article 9(2)(j) - Historical, statistical or scientific purposes	
4. Common Law duty of Confidentiality Compliance	Please tick the aspect of common law of confidentiality you are adhering to for this initiative (*please note the common law duty of confidentiality is not absolute*): ☐ Consent whether explicit or implied (implied meaning that the individual knows or would reasonably expect the proposed use of disclosure and has not objected) ☐ Authorised or required by law, for example, under statute, common law or legal proceedings ☐ Overriding public interest, for example, where a patient is contagious or the public is at risk, such that there is public interest in disclosure that overrides maintaining confidentiality.	
5. GDPR Principles compliance	Please tick the GDPR Principles that are applicable to this initiative and detail how you will comply: ☐ Principle (a) – lawfulness, fairness and transparency (please explain i.e. lawful – which legal basis, transparency – privacy notice) .... ☐ Principle (b) – data collected for specified, explicit and legitimate purposes (i.e. confirm the purpose the data will be used for) …….. …….. ☐ Principle (c) – adequate, relevant and limited to what is necessary (i.e. confirm how the data will be kept to a minimum) …… …….. ☐ Principle (d) – accurate and where necessary kept up to date (i.e. how will the integrity of the data be maintained) …….. …….. ☐ Principle (e) – storage limitation (i.e. data must not be kept for longer than is necessary, this may depend on the purpose – explain what measures are in place i.e. review and erase, anonymise if no longer required) ……	

DPIA Question	DPIA Response	Comments
	…… ☐ N/A	
6. Criminal Convictions & Offences Data – please state if you intend to process this data for this initiative / project / within a system?	☐ Yes ☐ No Please note this data is not covered by the GDPR. The DPA 2018 makes further provisions for processing this date when organisations are processing this other than law enforcement agencies.	

Section 5: Individual Rights

Informing individuals (Right to be informed): Please state how patients and / or staff will be informed / have been informed of the data collection and processing?	☐ Consultation, please provide details below ☐ Privacy Notice ☐ Other Information, please specify below
What are the arrangements for individual's to either object to their information being shared for direct care or to opt-out of the initiative for indirect care once they have been provided with the appropriate communication about it?	

Right of Access - Are there Subject Access Request Procedures for individual's to request access to the information held?	☐ Yes ☐ No ☐ Don't know Please detail:
If obtaining explicit consent, are their procedures in place to deal with individual's right for withdrawal of consent, right to erasure and the right to data portability?	☐ Yes ☐ No ☐ Don't know If yes, please specify policy / procedure name:
Other Individual Rights	Select which other Individual Rights apply: ☐ Right to Rectification ☐ Right to Erasure ☐ Right to Restrict Processing ☐ Right to Data Portability ☐ Right to Object ☐ Right in relation to automated decision making and profiling How will these be managed:
Marketing: **If a system, will it have the means to send marketing messages electronically?** If yes, please state what you are intending to send for marketing purposes:	☐ Yes ☐ No ☐ Don't know

Have individuals been informed of the marketing and the option to opt in to this?	
Automated Decision Making: Is automated decision making to be used within the system? If yes, please describe this process and reason for it and if there is any human intervention involved in decision making. Have individuals been informed of this process?	☐ Yes ☐ No ☐ Don't know

Section 6: Data Flow Mapping

Data Flow Mapping Table - Each flow of data for the initiative must be identified and documented to ensure this is securely undertaken and in accordance with GDPR and DPA 2018. This demonstrates the data that is being shared and with whom. Please complete the table below:

Flow	**Processed by or transferred from:**	**Processed by or going to:**	**Method of transfer**	**Security controls**	**Where will the data be stored following transfer**
e.g.GP Referral Letter	*e.g. GP Practice*	*e.g. NHS Trusts, Private Healthcare Supplier*	*e.g. secure email (NHSnet)* *Post*	*e.g. Encrypted email* *Limited as sent via Royal Mail*	*e.g. Saved in secure network folder* *Patients paper casenotes*

DPIA Question	DPIA Response	Comments
1. Will information be sent outside of the UK	☐ Yes, please go to question 2 ☐ No, please go to question 6	
2. Will information be sent outside the UK but within the European Economic Area (EEA)?	☐ Yes, please go to question 5 ☐ No, please go to question 3	
3. Will information be sent outside the EEA?	☐ Yes, please go to question 5 ☐ No	
4. Will the information be sent to the USA?	☐ Yes, please go to question 5 ☐ No	
5. Please state the country data will be sent too and the data security and protection arrangements in place.	Country: Security Arrangements:	
6. Is there an Information Sharing Agreement in place between the relevant parties that covers the processing agreements?	☐ Yes, please specify below: ☐ No	

Section 7: Organisational, Technical and Security Measures

1. Data Protection Registration Fee – have all the controller / processors & suppliers involved in the initiative paid their data protection annual fee?	☐ Yes, please state Name and ICO Registration Number below: ☐ No

2. Accreditation

Have all the parties completed an approved accreditation process in order to support compliance with the DPA 2018, GDPR, National Data Standards (Caldicott) and other national standards such as Cyber Essentials+, ISO 27001, Data Security and Protection Toolkit?

Partner Name	Accredtitation Scheme, Date Completed and Score	Audited and Outcome
i.e. GP Practice A	*DSPT submitted 15/03/2020 – Standards Met*	*Yes MIAA – Substantial Assurance Received*

3. Training

Is IG training provided for all partners and are all staff compliant?

Please also detail specific training required for the system?

Partner Name	Training Scheme Name	Compliance Information
e.g. GP Practice A *e.g. EMIS*	*Bluestream* *EMIS Health*	*Now an annual process for all staff (for DSPT compliance) – 96%* *All staff provided with refresh – 20/03/20*

Please note that staff should not access and use any system without any relevant system training

4. Incident Reporting

Do all partners have appropriate measures in place to report data security and protection incidents / breaches and share lessons learned?

☐ Yes
☐ No
☐ Don't know

5. Policies and Procedures Do all partners have IG / Data Security and Protection policies and procedures in place?	☐ Yes ☐ No ☐ Don't know
6. Contracts Are contracts (if required) in place with data processors and complaint with GDPR / DPA 2018? Are any sub-contractors used for this initiative?	☐ Yes ☐ No ☐ Don't know If contracts are used (e.g. between GP and system supplier) please state the partners of the contract below: Has the NHS England Standard Contract for Goods and Services been used for this? ☐ Yes ☐ No ☐ Yes ☐ No ☐ Don't know **What measures are taken to ensure processors comply**: *i.e. The current single processor, ABC, do not have direct access to the data and hold public assurance beyond reasonable doubt that they comply to the highest standards.*
7. Access Control and Rights for systems Who will have access to the system and the personal data? How will access be controlled and monitored?	Please detail:
8. Auditing	☐ Yes

Is there an audit trail for the system? Please can you describe briefly how the audit trail works?	☐ No ☐ Don't know
9. Data Quality Will data quality checks be implemented to ensure the data that is being received or shared is of good enough quality?	☐ Yes ☐ No ☐ Don't know Please detail:
10. Retention How has the the retention periods been decided? How long will the data be retained for in this initiative?	☐ As per the NHS Records Management Code of Practice for Health and Social Care ☐ Legal Statute, please state: ☐ Locally agreed decision ☐ Other, please state below:
11. Storage of Data Where will the data used for this initiative be stored / accessed?	☐ Within a paper based system stored securely ☐ Within a system / application stored on secure network ☐ Within a database / spreadsheet stored securely on network ☐ Other, please state below:
12. Disposal How will the data be securely destroyed / archived once it is	☐ Securely destroyed following local policies and national guidance ☐ Archived in secure environment. Please state reasons for archive and where the data will be stored below:

no longer required	
13. Back Up: <u>Applicable for IT systems only:</u> Are there secure and reliable back up processes in place for the data stored on the system? If yes, please briefly describe what these are.	☐ Yes ☐ No ☐ Don't know **Back up information** (*Please note you may need to contact IT Services for guidance regarding this question):*
14. Business continuity Do you have a Business Continuity Plan in place if the system and / or process fail or is unavailable for any reason? If yes, briefly describe what the business continuity plan will be:	☐ Yes ☐ No ☐ Don't know **BCP Process:**
Where a system is being implemented it is advised that the CCG's System Level Security Procedure (SLSP) is also completed; helps to demonstrate a considered and specific view of the range of security policy and management issues relevant to a system and that may encompass a range of technical, operational and procedural security topics.	

Section 8: Privacy Risks

The risks have been reviewed as part of the previous sections of this DPIA and should be highlighted, taking into account the below:

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular look at whether the processing could possibly contribute to:

- unauthorised access to data
- undesired modification of data
- disappearance of data
- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage

Include any sources of the risk i.e. person or non-human source that can cause a risk either accidentally or deliberately:

Specify any issues identified, recommendations and actions needed to secure the data if appropriate controls not in place within the risk assessment:

The risks should be reviewed, scored using the risk matrix below and incorporated into a risk register.

The level of risk is scored out of 25. A score of 0-5 is attributed to both the impact on the rights and freedoms of the individual, and the likelihood of those rights and freedoms being compromised. The two scores are then multiplied to create the composite risk score using the risk matrix below. This should be recalculated in the final columns to take into account proposed solutions/actions.

Privacy Risk Table

Risk	Description	Risk Score see matrix below			Proposed solutions/actions	Revised risk score see matrix below		
		Impact	Likelihood	Risk rating		Impact	Likelihood	Risk rating
Example - Risk 1	Unauthorised access to data – staff inappropriately accessing records	4	2	8	Document process that must be followed to ensure appropriate audit of staff access is undertaken and action as necessary	4	1	4

Refer to Appendix for guidance on Risk scoring.

Privacy Risks - Summary

☐ All privacy risks have been identified and actions have been identified to mitigate, accept or remove the risks. Where risks need to be monitored the Privacy Risk Table will act an action plan and be continually monitored by the DPIA completers.

☐ All privacy risks have been identified and actions completed to mitigate, accept or remove the risks.

☐ Not all privacy risks can be removed or reduced and the processing remains high risk, therefore the ICO must be consulted

NB: Where the processing remains high risk, that cannot be mitigated or remove, the ICO must be consulted:

DPO consulted: Yes ☐ No ☐ – DPO Advice Provided:

ICO Review required: Yes ☐ No ☐

If yes, ICO review outcome and date:

Screen 9: Additional Comments

Do you wish to supply additional comments about the system / asset? If yes please input comments in box:	☐ Yes ☐ No

Screen 10: Approval and Sign off

The Data Protection Impact Assessment must be approved and signed off by the relevant personnel, for example the Information Governance Board / DPO / Caldicott Guardian / SIRO.

DPIA Reviewed by:

Organisation	Name	Date	Signature

Approved by:

Organisation	Name	Date	Signature

Appendix - Glossary of Terms

Personal Data
Data which relates to a living individual which can be identified:
a) from those data, or
b) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller.

It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Special Category Data
Data consisting of information as to the:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

Health Data
This means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Anonymised Data
Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.

Pseudonymised Data
This is also sometimes known as reversible anonymisation. Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference. To be truly regarded as pseudonymised data the organisation must not hold the key to be able to reverse the anonymisation.

Processing
Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Large Scale Processing
The GDPR does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider:
- the number of individuals concerned;
- the volume of data;
- the variety of data;
- the duration of the processing; and
- the geographical extent of the processing.

Examples of large-scale processing include:
- a hospital (but not an individual doctor) processing patient data;
- tracking individuals using a city's public transport system;
- a fast food chain tracking real-time location of its customers;
- an insurance company or bank processing customer data;
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user data.

Individual professionals processing patient or client data are not processing on a large scale.

GDPR
General Data Protection Regulations

DPA 2018
Data Protection Act 2018

Data Controller
This means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor
This means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Consent
Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Implied consent
Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.

Explicit consent
Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients case notes) or in writing, to a particular use of disclosure of information.

Data Protection Officer
The GDPR requires all public authorities to nominate a Data Protection Officer (DPO). This role requires them to have reporting channels directly to the highest level of management and they must have the requisite professional qualities and expert knowledge of data protection compliance. They assist with the monitoring of internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for citizens and the Information Commissioner’s Office (ICO).

SIRO (Senior Information Risk Owner)
This person is an executive who takes ownership of the organisation‟s information risk policy and acts as advocate for information risk on the Board

IAO (Information Asset Owner)
These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they „own‟ and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.

IAM and IAA (Information Asset Managers / Administrators)
There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers

Information Assets
Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.

Information Risk
An identified risk to any information asset that the CCG holds. Please see the Information Risk Policy for further information.

Direct Marketing
This is “junk mail” which is directed to particular individuals. The mail which are addressed to “the occupier” is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.

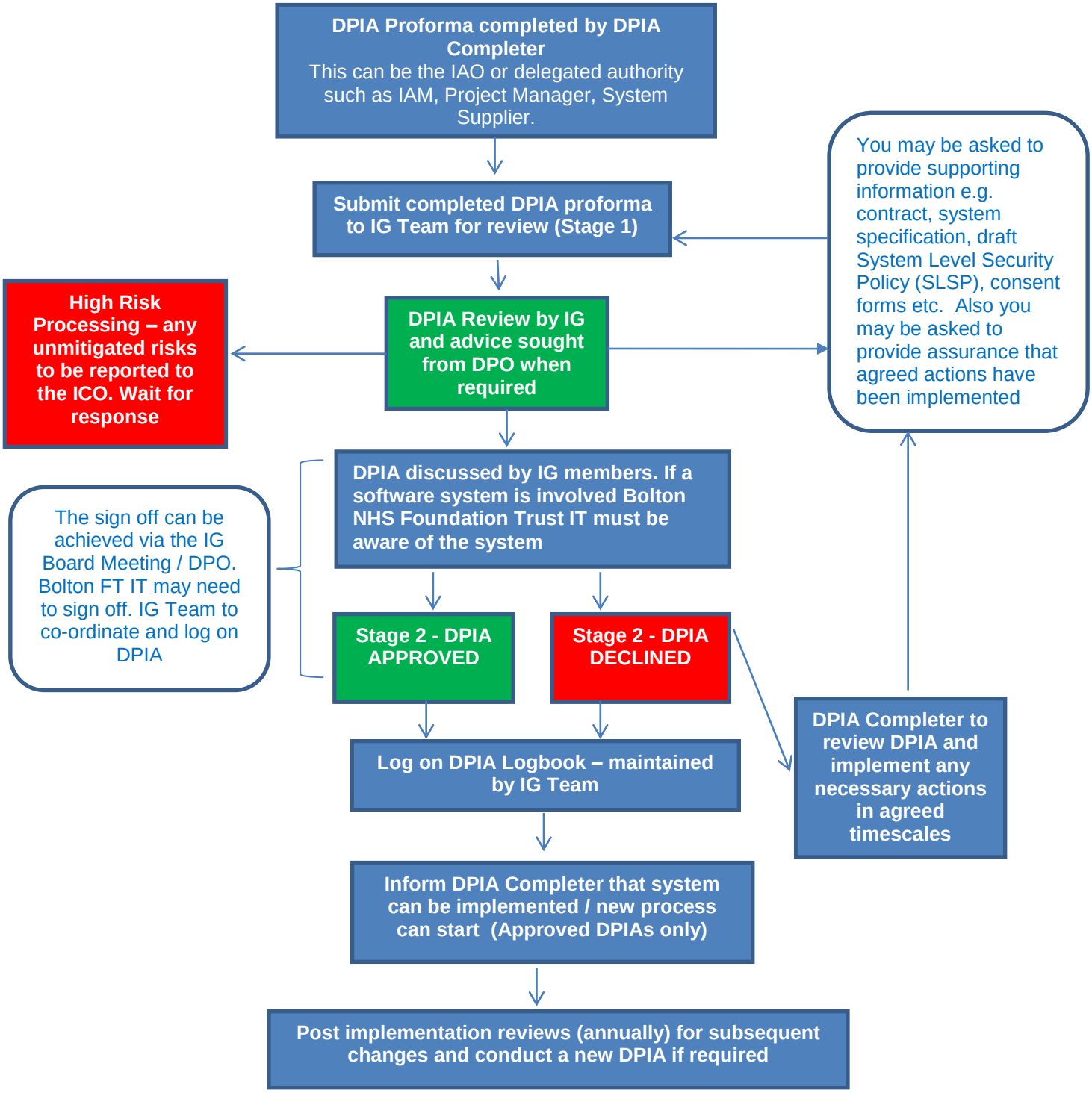
Automated Decision Making
Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned.

Retention Periods
Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.

Records Management: Code of Practice
Is a guide to the required standards of practice in the management of records for those who work within or under contract to health and care organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.

Appendix - Data Protection Impact Assessment Process Flowchart

The DPIA process can be displayed as a flowchart as per below. All stages of the process must be followed to ensure the system / asset adheres to confidentiality &information / IT security standards.



Appendix - How to score a Risk

	Impact (How bad it may be)		**Likelihood** (The chance it may occur)			**Risk Rating** **Likelihood x Impact = TOTAL RISK RATING**				
						Impact				
						1	2	3	4	5
5	Very High *(Will have a major impact)*	**5**	Almost certain *(almost certain to happen/recur; possibly frequently)*	**Likelihood**	5	**5**	**10**	**15**	**20**	**25**
4	Major *(highly probable it will have a significant impact)*	**4**	Likely *(Will probably happen/recur, but is not a persisting issue or circumstance)*		4	**4**	**8**	**12**	**16**	**20**
3	Moderate *(Likely to have an impact)*	**3**	Possible *(Might happen or recur occasionally)*		3	**3**	**6**	**9**	**12**	**15**
2	Minor *(May have an impact)*	**2**	Unlikely *(Do not expect it to happen/recur, but it is possible it may do so)*		2	**2**	**4**	**6**	**8**	**10**
1	Negligible *(Unlikely to have any impact)*	**1**	Rare *(This probably will never happen/recur)*		1	**1**	**2**	**3**	**4**	**5**

Total Risk Rating	**Risk**
1-3	Low
4-6	Moderate
8-12	High
15-25	Extreme