NHS
Salford
Clinical Commissioning Group

Data Protection Impact Assessment (PIA) Proforma

Reference: MS-Teams
PIA Title: MS Teams
Version: 1.0
Date: May 2020

DOCUMENT CONTROL PAGE	
Title	Data Protection Impact Assessment Proforma
Version	2
Date	April 2018
Review	April 2020

Why do I need to complete a Data Protection Impact Assessment?

Data protection impact assessments (DPIAs) help organisations identify, assess and mitigate or minimise privacy risks with data processing activities. They're particularly relevant when a new data processing process, system or technology is being introduced.

DPIAs also support the accountability principle, as they help organisations comply with the requirements of the Data Protection Regulation and demonstrate that appropriate measures have been taken to ensure compliance.

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

Please note the template is constantly being changed / updated to meet new requirements so always make sure you use the latest version.

When do I complete a Data Protection Impact Assessment?

If you are doing any of the following:

GDPR introduces a new obligation to do a DPIA before carrying out types of processing likely to result in high risk to individuals' rights and freedoms.

- setting up a new process whether you are using personal confidential data (PCD) or not, then a DPIA should be completed and filed with the project paperwork
- changing an existing process which changes the way personal confidential data is used
- procuring a new information system which holds personal confidential data

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

Who needs to complete a Data Protection Impact Assessment?

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

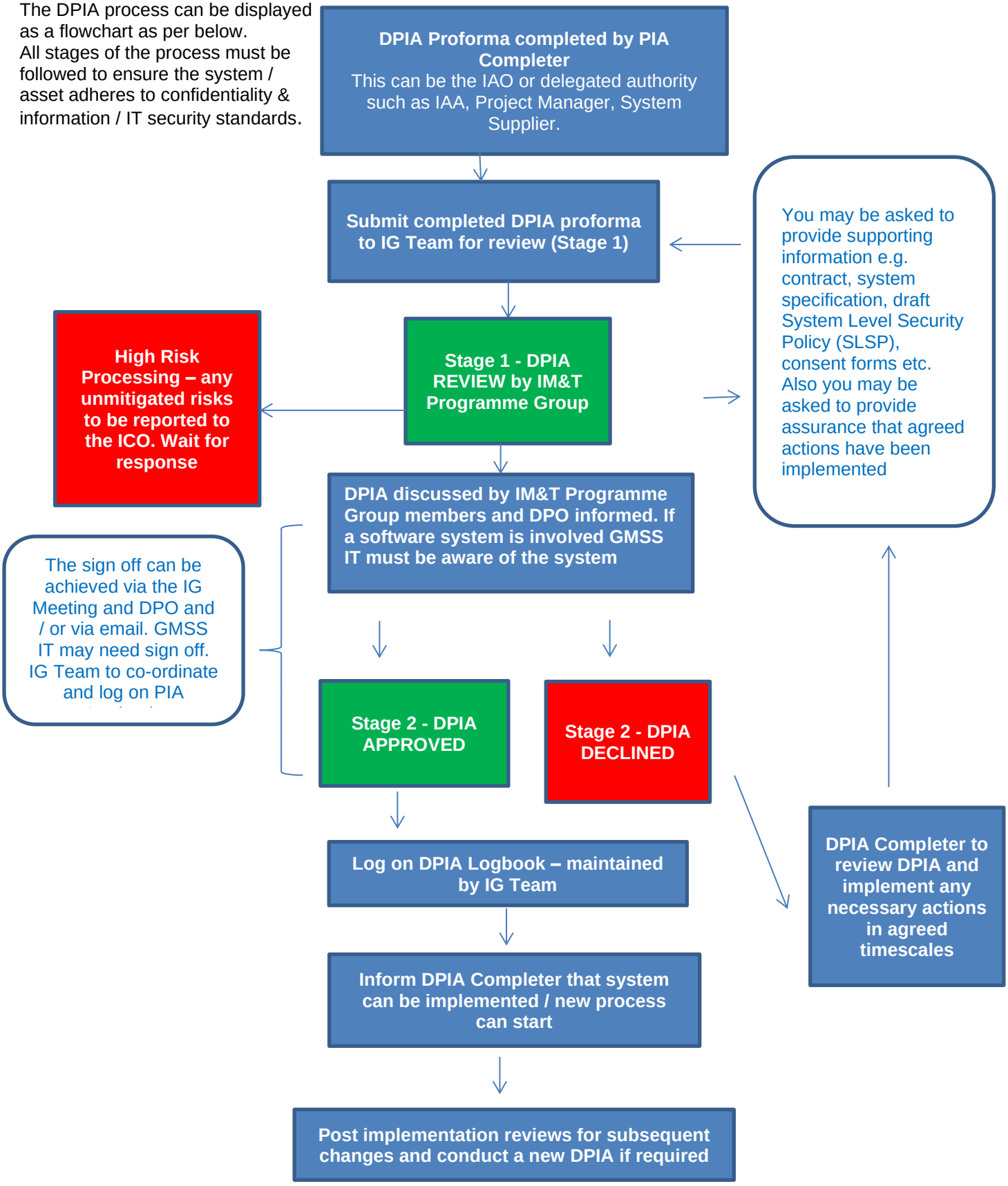
DPIA Process Flowchart

Please complete each section (where applicable) with as much information as possible. For example, a key piece of information is who the Information Asset Owner and Information Asset Administrator will be for a system / asset.

The following flowchart highlights the steps once the DPIA has been completed until either approval and / or rejection decision has been reached.

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.



Important

By completing this Data Protection Impact Assessment, all parties associated with the DPIA agree to adhere to the Data Security & Protection Toolkit requirements and have Data Security and Information Security Policies in place as follows:

- System Level Security Policy including Business Continuity Plan
- Data Protection Procedure/Policy
- Completion of Data Security mandatory training
- Incident Reporting Procedures
- Safe Transfers of Information Procedure
- Information Asset Register
- Data Flow Mapping Register

The list above is not exhaustive.

In the event of an incident and failure to have the above may incur a larger monetary penalty being levied upon you by the Information Commissioners Office (ICO).

Screen 1: PIA Completed by:

Organisation	**Name**	**Date**	**Signature**
Salford CCG	Ruth Quinn	05/05/2020	R A Quinn
Click here to enter text.	Click here to enter text.	Click here to enter a date.	

For completion by: IG/Approval Group

Approved – no actions required	☒	Click here to enter a date.
Approved with action plan	☐	Click here to enter a date.
Declined (give reason)	☐	Click here to enter text. Click here to enter a date.

Screen 2: Basic Information

PIA Completer Name: *(please note this can be Project Manager / IAO / IAA or whoever has been requested to complete the proforma):*	Ruth Quinn
Department:	IG
Email:	ruth.quinn@nhs.net
Telephone No.:	Click here to enter text.
New System / Process Name:	Microsoft (MS) Teams
New System Supplier Name: **(if applicable):**	Microsoft
Date System due to go live (if applicable):	March 2020
Project Proposal / Purpose for completing DPIA:	Microsoft Teams (MS Teams) is a unified communication and collaboration platform that combines workplace chat, video meetings, file storage, and application integration. MS Teams and its integration with many other Office365 applications has been approved by NHS Digital (NHSD).The NHSD provided installation of MS Teams comes with a number of pre-installed Applications which are considered within the scope of this DPIA. The CCG have implemented MS Teams as a staff collaboration tool, to support staff in working together remotely through: • audio / video conferencing - 1:1s & meetings across multiple sectors / organisations and internal • chat messaging - 1:1s and group chats. Also used within audio / video calls, i.e. asking questions of the chair / speaker etc. • file sharing – to share documents, although the majority of staff save documents on the N drive within their departmental folders and can access them through those means, so use of file sharing for internal staff may be minimal

	• collaborative file editing - used to rapidly update a single document. MS Teams is configured to facilitate this activity within GMSS and moving forward Salford Councils ICT's Infrastructure and is installed across the CCG patch. It is being provided by via the NHSmail environment. The use of MS Teams is of paramount importance to aid remote working across the CCG, particularly during the current pandemic. MS Teams can be used across a multitude of devices and therefore supports agile working, up to and including off-site working. MS Teams will be set up on user's laptops. Not only will MS Teams allow staff to continue to work but other benefits include: Communication, convenience and efficiency are all delivered in allowing agile working as described Cost savings are envisaged as the audio/video conferencing provides an alternative to telephony. Public health and the provision of healthcare are supported by facilitating more effective use of staff resources, including through remote home working. E.g. in the context of COVID-19 staff are able to avoid coming to site and exposing themselves to public health risks. **MS Teams – Audio / Video Conferencing.** Those who set up meetings are able to manage who participates in their meetings and who has access to meeting information. The user becomes the administrator and can decide who from inside and outside the CCG can join the meeting, invitees wait in a 'lobby' for the administrator to let them in. Furthermore, administrators can remove participants during a meeting, designate "presenters" and "attendees," and control which meeting participants can present content. And with guest access, people can be added from outside the CCG but control over the data is retained. Moderation allows the user to control who is and isn't allowed to post and share content. And advanced artificial intelligence (AI) monitors chats to help prevent negative behaviours like bullying and harassment. There is a recording facility which may be useful for users if they want to record training sessions for example. Before a user starts recording it will ask them to confirm they are abiding by the organisations policy, users click accept and the recording starts. When the recording finishes it is uploaded to Microsoft Stream account of the user, the user who initiated the recording, no one else will see this at this point. Once the meeting has finished the video can then made available to the whole group within the chat facility of the meeting. As the video is saved to the users Microsoft Stream account the link can also be shared to specific individuals or the whole organisation. Stream is an enterprise video service where users in an organisation can upload,

	view, organise and share videos securely. The data / recordings if not deleted by the user will be saved in the same data centre as the users files / documents / chats. CCG staff must be mindful of the personal data they process (discuss and record) via audio / video conferencing, keeping identifiers to a minimum if personal data needs to be discussed. **MS Teams – File Sharing Capabilities** *Uploading /Sharing files on Microsoft Teams* Microsoft Teams allows users and teams to upload files in a secure file structure. This involves both a personal 'OneDrive' file storage (which is roughly equivalent to a user's personal drive on the CCG / IT desktop). It also includes structured file sharing across 'Teams' of CCG staff. Personal Files – A user is able to store files that are visible and accessible only by himself / herself via OneDrive. Storing files onto OneDrive is the equivalent to storing a file on to a local 'personal drive.' *Shared Files and Team Structures* Users may store files on a designated private 'Team' which is a shared environment. These files will be accessible by all members within the team via SharePoint. This 'Team' tab provides the functionality to serve as central repositories for information required to be shared between members of a team. *Sharing files over ad hoc chats* Files may also be shared outside of a team within a 'chat' environment where files will be visible, available and accessible by all members within the 'chat' via SharePoint. Chats may be established with any other member of the organisation, allowing CCG staff to share files across different divisions, departments etc. Sharing a file on an individual chat will lead to a SharePoint being established within that chat's environment. A 'Team' and/or a 'Chat' on Microsoft Teams allows members to collectively work on and store files on a shared environment via SharePoint (i.e., in a manner comparable to a shared drive). Therefore, managers must be aware that every 'Team' and 'Chat' member will have visibility of the uploaded files. Storing files on a 'Team' SharePoint is the equivalent of saving a file onto a local 'shared drive' (i.e., an 'S:' drive). It is recommended that the Team SharePoint is used as the primary file structure for the team's documents. Sharing files over an individual 'Chat' is similar to sharing a document over email as an attachment, except that all members of that chat group have visibility and write-access to the files shared. It is recommended that files shared over Chats are worked on in situ and then stored centrally in the

	relevant Team file structure. It is important to remember that whenever a file is shared over a Team or Chat group, it is available and accessible to all members of that group. Therefore, CCG staff must be mindful of the data being shared and the appropriateness of access being provided to these staff. Data shared should be minimal for the purposes of sharing and access limited to those that require it. CCG staff must be mindful of the personal data contained within any documents they share via chat and video conferencing, particularly as this information is saved on the OneDrive. Where possible redact personal data before sharing. **MS Teams – Screen Sharing Functionality** Users are able to show one another their screens. This will be useful if presenting or referring to a document. CCG staff must ensure that if they share their screen that contains personal data, that they will inform the attendees in advance. As remote / home working is currently taking place, this will give the attendees a chance to alter their position of the screen (if in view of others at home) or move location. CCG staff are reminded to only share the minimum amount of personal data and to be aware of their audience. **The use of Personal Data within MS Teams (available to CCG Staff and Microsoft)** Majority of users will be processing data which will be business data and some potentially classed as business sensitive / confidential. Much of the information held in meeting chats etc. can be regarded as 'process notes' not constituting personal data. It is recognised that the CCG have teams that handle personal data i.e. NHS Funded Care Team, Safeguarding, Medicines Optimisation, Complaints and Serious Incidents. It is expected that these teams will need to discuss patients in their care via audio / video conferencing, however they cannot be recorded (this is not being enabled) so the information will be discussed in real time. These teams are able to 'file share' they will be reminded to only file share when absolutely necessary when the file contains personal data. They will be reminded to regularly delete the files from the 'OneDrive' folder within Teams. The same will apply to these teams using the 'chat messaging' facility, this can be used by the Teams but not to discuss identifiable individuals / patients. Where 'collaborative file editing' is used again CCG staff should be mindful of where the copies are saved and remove when they are no longer required for editing. These files although not viewable to other users are stored within Microsoft Azure, data centres are based in the UK –

	London and Cardiff. In the main MS Teams will be used as conduit / platform for CCG to staff communicate, data will pass through and the majority will not be stored i.e. audio / video calls. However, chat messaging and file sharing data will be stored within MS Teams – CCG business data and potentially limited personal data. Whilst MS Teams is not a patient administration system, it supports a number of applications and a file structure in which patient data may be held and processed. This is subject to access controls in line with equivalent Trust file servers and comes under the support of patient care. Microsoft Teams, as a cloud-based service, processes various types of personal data as part of delivering the service, above mentions personal data relating to patients, however this may also include personal data relating to the users / staff members. This personal data includes: • Content - meetings and conversations chats, voicemail, shared files, recordings and transcriptions – patient data and confidential data may be shared here too. • Profile Data - data that is shared within the CCG about the user / staff member. Examples include E-mail address, profile picture, and phone number. • Call History - a detailed history of the phone calls the user make, which allows the user to go back and review their own call records. • Call Quality Data - details of meetings and call data are available to the CCG's IT system administrators. This allows IT administrators to diagnose issues related to poor call quality and service usage. • Support/Feedback Data - Information related to troubleshooting tickets or feedback submission to Microsoft. • Diagnostic and Service Data - Diagnostic data related to service usage. This personal data allows Microsoft to deliver the service (troubleshoot, secure and update the product and monitor performance) as well as perform some internal business operations, such as: o Determine revenue o Develop metrics o Determine service usage o Conduct product and capacity planning To the extent Microsoft Teams processes personal data in connection with Microsoft's legitimate business operations, Microsoft will be an independent data controller for such use and will be responsible for complying with all applicable laws and controller obligations. This DPIA is considered from a data security perspective, considering the personal data and business confidential data

<table>
<tr><td></td><td>that may be processed by the CCG.</td></tr>
<tr><td>Link to any wider initiative:
(if applicable)</td><td>Enter links to any wider initiatives if applicable</td></tr>
<tr><td>Information Technology involvement</td><td>List any applicable electronic systems/software to this initiative (current and/or new):
<table><tr><th>System name</th><th>Used by e.g. organisation and dept.</th><th>Parties/system supplier</th></tr><tr><td>MS Teams</td><td>CCG</td><td>Microsoft</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><tr><td></td><td></td><td></td></tr></table></td></tr>
<tr><td>Are any other organisations are involved in this initiative?</td><td>NHS Digital, GMSS and moving forward Salford CCG Council IT</td></tr>
<tr><td>Confirm all relevant organisations have or are working towards cyber essentials</td><td><table><tr><th>Organisation/Parties/ system supplier</th><th>Cyber essentials Y/N
Working towards/cyber compliance defined under terms of contract</th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table>Taken from https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/06/microsofts-commitment-privacy-security-microsoft-teams/

We protect your data and defend against cybersecurity threats
As a leader in security, Microsoft processes more than 8 trillion security signals every day and uses them to proactively protect you</td></tr>
</table>

	from security threats. In Teams, we encrypt data in transit and at rest, storing your data in our secure network of datacenters and using Secure Real-time Transport Protocol (SRTP) for video, audio, and desktop sharing. Also, refer to: https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview
Is this initiative in line with or achieving national or local guidance/ strategy or mandate?	If yes give details

Screen 3: Screening Question

Documenting here which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template

		Yes	No	Unsure	**Comments** *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
a)	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?	☐	☒	☐	Click here to enter text.
b)	Will the initiative involve the collection of new information about individuals?	☐	☒	☐	Click here to enter text.
c)	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not	☐	☒	☐	Click here to enter text.

	currently used?				
d)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?	☒	☐	☐	MS Azure – only for personal data that is stored within MS Teams most likely by using files, although the CCG will ask staff keep this to a minimum
e)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐	☒	☐	Click here to enter text.
f)	Does the initiative involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition	☐	☒	☐	Click here to enter text.
g)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐	☒	☐	Click here to enter text.
h)	Will the initiative compel individuals to provide information about themselves?	☐	☒	☐	Click here to enter text.

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

Screen 4: Contact Information

Project Management Details	
Project Manager:	Click here to enter text.
Project Manager Email:	Click here to enter text.
Project Manager Telephone No.:	Click here to enter text.
Information Asset Owner (IAO) Details	
IAO Name:	Click here to enter text.
IAO Title:	Click here to enter text.
IAO Department:	Click here to enter text.

IAO Email:	Click here to enter text.
IAO Telephone Number:	Click here to enter text.
Information Asset Administrator (IAA) Details	
IAA Name:	Click here to enter text.
IAA Title:	Click here to enter text.
IAA Department:	Click here to enter text.
IAA Email:	Click here to enter text.
IAA Telephone Number:	Click here to enter text.

Screen 5: Personal Confidential Data Items

	Yes	No	If Yes complete the rest of the form. If No go to screen 7
Is the project collecting Personal Confidential Items	☒	☐	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Personal details	Information that identifies the individual and their personal characteristics	Check all that apply: ☑ Forename(s) ☑ Surname ☑ Address ☑ Postcode ☑ Date of Birth ☑ Age ☑ Gender ☑ Physical description ☑ Home Telephone Number ☐ Mobile Telephone Number ☐ Other Contact Number ☑ Email address ☑ GP Name and Address ☑ Legal Representative Name (Next of Kin) ☑ NHS Number ☐ National Insurance Number ☐ Photographs/Pictures of persons ☐ Other – if this is ticked please list 'Other' personal data items to be processed below: See attached	The personal data items may differ depending on the departments within the CCG but this is based on the NHS Funded Care Team who are the team who will process the majority of personal data. Safeguarding, Medicines Optimisation, Complaints and Serious Incidents may process limited personal data. The majority of departments will be processing business confidential data that does not contain personal data.
Physical or mental health or condition	Information relating to the individuals physical or mental health or	☑ Yes ☐ No ☐ Not applicable	For NHS Funded Care Team, Safeguarding

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
	condition. NB. For mental health this would include the mental health status i.e. whether detained or voluntary under the Mental Health Act.	List any data items below or attach as an appendix: Click here to enter text.	
Sexual identity and life	Information relating to the individuals sexual life	☐ Yes ☐ No ☑ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Family lifestyle and social circumstances	Information relating to the family of the individual and the individuals lifestyle and social circumstances	☐ Marital/partnership status ☐ Carers/relatives ☐ Children/dependents ☐ Social status e.g. housing ☐ Not applicable ☑ Other - please specify below: Click here to enter text.	Potentially Safeguarding team
Offences including alleged offences	Information relating to any offences committed or alleged to have been committed by the individual	☐ Yes ☑ No ☐ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Potentially Safeguarding team
Criminal proceedings, outcomes and sentences	Information relating to criminal proceedings outcomes and sentences regarding the individual	☐ Yes ☐ No ☑ Not applicable List any data items below or attach as an appendix:	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
		Click here to enter text.	
Education and training details	Information which relates to the education and any professional training of the individual	☐ Education/training ☐ Qualifications ☐ Professional training ☑ Not applicable ☐ Other - please specify below: Click here to enter text.	Click here to enter text.
Employment details	Employment and career history	☐ Employment status ☐ Career details ☑ Not applicable ☐ Other - please specify below: Click here to enter text.	Click here to enter text.
Financial details	Information relating to the financial affairs of the individual	☐ Income ☐ Salary ☐ Benefits ☑ Not applicable ☐ Other – please specify below: Click here to enter text.	Click here to enter text.
Religious or other beliefs of a similar nature	Information relating to the individuals religion or other beliefs	☐ Yes ☐ No ☑ Not applicable List any data items below or attach as an appendix: Click here to enter text.	Click here to enter text.
Trade union membership	Information relating to the individuals membership of a trade union	☐ Yes ☐ No ☑ Not applicable List any data items below or attach as an appendix:	Click here to enter text.

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
		Click here to enter text.	
You must confirm that the data items you have ticked above are relevant and necessary to your project and there is a justified reason for it –if they are not you must amend the above selections to remove those items not relevant/necessary			
Confirm ☐			

Screen 6: Legal Basis for Processing the Data

Is the initiative delivering 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 Q1)** ☐ **N/A (go to screen 7)**

1a. If not Direct care, what is it delivering and how is the consent being obtained	Indirect care • Commissioning ☐ • Monitoring Health and social care ☐ • Public health ☐ • Research ☐ • Other ☐ specify ……
1b. What is the legal basis that permits you to carry this out for indirect care?	Legal basis: • Explicit consent ☐ • Section 251 ☐ • Other legal gateway (please state) ☐ Personal data and Special Category Data will be processed by NHS Funded Care Team, Safeguarding, Medicines Optimisation, Complaints via MS Teams therefore an legal basis from Article 6 is required and a condition from Article 9. NHS Funded Care Team, Safeguarding and Medicines Optimisation Article 6: (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. Article 9: (h) Health or social care (with a basis in law) (i) Public health (with a basis in law) Complaints Dept: Article 6 (1)(a) – Consent And Article 9 (a) – Explicit Consent (h) - Health or social care (with a basis in law) How will the CCG comply with the GDPR Principles: Principle (a) – lawfulness, fairness and transparency Lawfulness – Lawful bases have been applied (as detailed above): Personal Data - Article 6(1)(e) and Special Category of Data - Article 9(2)(h) of GDPR Common Law Duty of Confidentiality – Implied Consent Fairness and Transparency - In order for the data processing to be fair and transparent, the proposed use must be expected by the individual. This is documented on the Patient Privacy Notice which is available

	on the CCG's website. Principle (b) – collected for specified, explicit and legitimate purposes The purposes for processing are detailed in the Privacy Notice and this personal data is not used for any other purpose than for use for what the patients currently expects. Principle (c) – adequate, relevant and limited to what is necessary Staff will only share personal data within a team / meeting on a need to know basis, personal data will be kept to a minimum. Principle (d) – accurate and where necessary kept up to date Staff will ensure any personal data they process / share is up to date. Principle (e) – kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed The CCG has its own retention schedules for electronic data it keeps about individuals, normally in accordance with Appendix 3 of the Records Management Code of Practice for Health and Social Care 2016. However, staff will be advised to delete the data from MS Teams as soon as they can and no longer required, as this information will also be saved in the N drive if they need to refer to it in the future. Principle (f) - processed in a manner that ensures appropriate security of the personal data Access is granted via the user's NHSmails credentials. Any files that are stored via OneDrive can only been seen and accessed by themselves. This information will also be stored in MS Azure's data centre in the UK. MS will restrict access by Microsoft personnel and subcontractors. **Individual Rights:** Refer to the CCG's Patient Privacy Notice for further guidance.
2. 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 appropriate communication about it?	This is not applicable for MS Teams, as is the mechanism / tool being used to process personal data by CCG staff. As an aside patients can contact the CCG to opt out of the processing, however if this is for Direct Care the CCG can decline the request if it is for the best interests of the patients.

Informing individuals: How have patients and / or staff been informed of the data collection and processing?	Please state: There is no requirement to inform individuals that the CCG will be using MS Teams to potentially process some of their data as this is just a mechanism to process the data.

Information Sharing within UK:

Will personal confidential data be shared with any other organisation?

If yes, please state who the information will be shared with and how

☒ Yes ☐ No

From Originator Organisation:	Data sent to via:	To Receiving Organisation:
CCG/GMSS	MS Team	Microsoft Azure

Is the information from receiving organisation sent back to originating organisation. If yes, please state how the information is transferred back:

From Receiving Organisation:	Data sent back via:	To originating organisation:
Microsoft Azure	MS Team	CCG/GMSS

Information Sharing outside the UK:

Will Personal Confidential Data be sent outside the UK?

If yes, please state who the data will be sent to and how?

Will Personal Confidential Data be sent outside the European Economic Area (EEA)?

If yes, please state who

☒ Yes

☐ No

Microsoft Azure potentially hosts data externally to the EU/EEA. However, this will only ever be the case where appropriate third country transfer mechanisms are supported (through BCRs or Adequacy Decisions e.g. EU-US Privacy Shield certification.) Microsoft Corporation and its subsidiaries are Privacy Shield certified. The Teams application uses specific Azure blob, table, and queue storage (collectively referred to as the Teams substrate). Files are stored in SharePoint and OneDrive for Business, and meeting recordings are stored in Stream, all of which in turn use Azure storage. However, MS Teams currently use UK data centres in London and Cardiff.

the data will be sent to and how? Have data protection checks been undertaken to ensure that the non EEA country has adequate data protection / information security? If yes, please state what checks have been made: **Sending data to the USA**	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No

Screen 7: Asset / System Information

ICO Notification: If a system is being used, is the Supplier registered with the Information Commissioners Office (ICO). If yes, please state their registration number:	☐ Yes ☐ N/A ☐ No [ ]
DSPT Toolkit: Has the Supplier / Third party completed an Data Security and Protection Toolkit (DS&P) Assessment & that has been internally/externally audited and/or has ISO27001 accreditation? If so, which version and to what level? Please provide evidence.	Data Security and Protection Toolkit completed: ☐ Yes ☐ No DS&P Toolkit audited ☐ Yes ☐ No ISO 27001 Accreditation ☐ Yes ☐ No Evidence: Click here to enter text.
Contract: Has the supplier (if applicable) signed the relevant contract (containing the Information Governance clauses) e.g. NHS E contract / SLA with IG Clause. If yes, please state which contract type they have signed up to:	☐ Yes ☐ No ☐ N/A [Click here to enter text.]

Asset / System Operation: Does the asset use privacy invasive technologies for staff and / or patients? See **Glossary** for advice	☐ Yes ☐ No
If yes, please state the technology being used:	Click here to enter text.
Will the asset / system process new / different personal confidential data items which have not been processed previously?	☐ Yes ☐ No
If yes, please state the new personal confidential data items to be processed:	Click here to enter text.
Will the asset / system involve new or changed identity authentication requirements that may be intrusive for staff and / or patients?	☐ Yes ☐ No
If yes, please state the new identity authentication requirements:	Click here to enter text.
Marketing: Will the asset / system send marketing messages by electronic means?	☐ Yes ☐ No
If yes, please state what you are intending to send for marketing purposes:	
Have individuals been informed of the marketing and the option to opt in?	☐ Yes ☐ No

	Click here to enter text.
Automated Decision Making: Is automated decision making to be used within the asset / system? If yes, please describe this process and reason for it	☐ Yes ☐ No Click here to enter text.

Screen 8: System Security and Functions – only to be completed for systems

Pseudonymisation / Anonymisation: Can personal confidential data be anonymised or pseudonymised using the system / asset?	☐ Yes ☐ No
Data Quality: How will the personal confidential data be kept up to date and checked for accuracy?	Click here to enter text.
Access: Who will have access to the system and the personal confidential data? How will levels of access be decided.	Click here to enter text.
Auditing: Is there an audit trail for the system?	☐ Yes ☐ No
Storage of data: Where will the system information be stored securely?	☐ Within a paper based system stored securely ☐ Within a system / application stored on secure network ☐ Within a database / spreadsheet stored securely on network ☐ Other Click here to enter text.
Retention: What are the retention periods for the information processed in the system?	Click here to enter text.
Disposal: How will the personal confidential data be disposed of when this is no longer required?	Click here to enter text.

Training: Each party to confirm that information governance training is in place and all staff with access to personal data have had up to date training	☐ Yes ☐ No

Additional Comments

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

Signed off by:

Organisation	Name	Date	Signature
Salford CCG	IM&T Programme Group	26/05/2020	R A Quinn
Click here to enter text.	Click here to enter text.	Click here to enter a date.	

Glossary of Terms

Item	Definition
Personal Data	This means 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	This means personal 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
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.
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.
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.
IAA (Information Asset Administrator)	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
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.
Anonymity	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.
Pseudonymity	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.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and

	video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
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: NHS 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 NHS 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.
Data Protection Legislation	This Legislation defines the ways in which information about living people may be lawfully used and handled. The aim is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must: with those purposes. loss, destruction or damage. unless that country or territory protects the rights and freedoms of the data subjects. These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.