Royal Free London
NHS Foundation Trust

Data Protection Impact Assessment (DPIA) template

Section A – project details

Project Name	**Video Consultation Pilot (Attend Anywhere)**
Organisation(s)	Royal Free London NHS Foundation Trust
Project lead (staff member completing the template)	[redacted]
Job title	Programme Manager
Date completed	14/10/19
Phone	[redacted]
E-mail	[redacted]

Introduction - What is a Data Protection Impact Assessment?

Patients have an expectation that their privacy and confidentiality will be respected at all times during their care and beyond. It is essential therefore, when considering or implementing any new initiatives, that the impact of the collection, use and disclosure of any patient (or staff) information is considered in regards to the individual's privacy. Carrying out a Data Protection Impact Assessment (DPIA) is a systematic way of doing this.

A DPIA is a process that helps an organisation to identify privacy risks and ensure lawful practice when a new project is designed or changes are made to a service. The purpose of the DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. It is a particularly useful tool for organisations to identify privacy risks and ensure lawful practice use when:

- Planning a new information sharing initiative such as working with new partners or in different ways;
- Introducing new IT systems for collecting and accessing personal data;
- Intending to use personal data for new uses. *(for more examples see page 4, 1.3)*

Why is this necessary?

From 25 May 2018 the GDPR introduces a new obligation on organisations to undertake a DPIA before carrying out processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk which you cannot mitigate, the trust must consult the Information Commissioners Office (ICO) for advice.

A DPIA helps an organisation to see things from the patient's (or staff members) point of view. It is their data that is being used and usually their choice about how and why it will be used. "No decision about me, without me" is the vision for the patient-centred NHS. Understanding the impact to the individual(s) personal data enables the system to be designed around their legal rights and expectations of confidentiality.

A DPIA also checks organisational compliance against the legal framework such as the Data Protection Act and General Data Protection Regulation (GDPR), see also privacy risks below.

What are privacy risks?

Privacy risks include the following:

- Risks to individuals or other third parties (for example, misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency).
- Compliance risks e.g. breach of the Data Protection Act (DPA) or GDPR
- Risks to the organisation (for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public).

Where do I start? The DPIA process

1. Fill out the **contact details at the top of page 1, section A**. The project lead should be nominated to co-ordinate the DPIA process.

2. Complete the DPIA screening process - see **below section B**. Answering the screening questions will identify whether or not the proposed initiative will impact on patient privacy and whether or not you need to complete a full DPIA. The screening questions are designed to give you a quick sense of the scale of the privacy issues that you may be facing.

3. If you answer "yes" or "unsure" to any of the screening questions in the table, you will need to undertake the DPIA – see **sections C to E on pages 4 to 13**. You may find it helpful to seek assistance from the trust's Data protection officer / IG team to help you with the process.

4. Once completed send the document to for **review and approval section F**.

Section B - DPIA screening questions

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. This will also assist in ensuring that the investment the organisation makes is proportionate to the risks involved.
Tip – imagine this initiative involved the use of your own information or that of a relative.

		Yes	No	Unsure	Comments
1	Will the initiative use systematic and extensive profiling or automated decision-making to make significant decisions about people?	☐	☒	☐	
2	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?	☐	☒	☐	
3	Will the initiative involve the collection of new information about individuals?	☐	☒	☐	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐	☒	☐	

5	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?	☒	☐	☐	Patients are given a choice about whether to use the video service and consent is obtained
6	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐	☒	☐	
7	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?	☒	☐	☐	No recording of the video appointment is saved
8	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐	☒	☐	
9	Will the initiative process personal data which could result in a risk of physical harm in the event of a security breach?	☐	☒	☐	

If you answered **No** to all of the above, and you can evidence/justify your answers in the comments box above, you do not need to continue with the DPIA as it will not apply to your initiative. Should the initiative change to incorporate informational privacy at any point in the future you will need to complete the screening questions again.

Conducting a full DPIA

1.1 What should a DPIA include?

In simple terms the DPIA should:

- Set out the aims or objectives of the initiative
- Explain why the DPIA is necessary (the initial screening questions at the beginning of the template will enable this to be quickly identified)
- Document the data flows in terms of, what data is being processed, where it is coming from and who it is going to
- Identify the risks to individual's privacy in terms of security, and as potential threats to confidentiality, integrity or availability
- Clarify the legal basis
- Identify and evaluate the privacy solutions (how can you reduce or remove the risk?)
- Sign off and record the DPIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders, as needed, throughout the process.

[1] Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

1.2 Who should be part of the DPIA team needed to complete the template?

For the DPIA to be effective it needs input from people with a range of expertise, skills and authority. Important features for members of the team include:

- An understanding of the project's aims and the organisation's culture;
- Authority to influence the design and development of the project and participate in decisions;
- Expertise in privacy and compliance matters;
- Ability to assess and communicate organisational risks;
- Ability to assess which privacy solutions are feasible for the relevant project; and
- Ability to communicate effectively with stakeholders and management.

1.3 Does my project need a DPIA?

From 25 May 2018 the GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. A DPIA is suitable for:

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action
- Using existing data for a new and unexpected or more intrusive purpose
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system
- A new database which consolidates information held by separate parts of an organisation
- Legislation, policy or strategies which will impact on privacy through the collection of personal information, or through surveillance or other monitoring
- Long standing databases where the privacy impact may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues.

Section B - Full DPIA template

Background Information

Project/Change Outline - What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required.
It is planned to pilot video clinic consultations to demonstrate proof of concept and to trial the video consultation software, Attend Anywhere. Patients will be booked into a specific video appointment slot and instead of travelling to attend a face-to-face appointment they will have a consultation at a more convenient location for them (ie home / work / private space elsewhere) by logging in to the Attend Anywhere platform using a laptop, tablet, PC or smartphone. The pilot will initially be conducted in the following specialties: • Respiratory • Gastroenterology • Paediatric gastroenterology • Vascular surgery

Attend Anywhere is a web browser based application. To access their appointment, patients enter the clinic's online waiting area using a secure link via their smartphone or tablet.

Patients do not need to set up any kind of user account: they will be provided with a link in their appointment letter and reminder text that is specific to the specialty clinic. They copy and paste (or click) on the link and then click the 'Start video call' button and follow the prompts. The personal information they provide on entry is not stored beyond the end of the call.

Clinicians sign into the Attend Anywhere Management Platform from a web browser, select the Waiting Area that relates to their clinical service, then selects a patient from the queue.
The clinician is notified when a patient has arrived, and joins the consultation when ready.

Security of the platform

- The patient waits in their own private video room until an authorised healthcare professional is ready to join them. The consultation will occur in a private video room, as if meeting face-to-face. It doesn't matter if a clinician is running overtime with another patient, as there is no chance of people running into each other. The room is deleted after the consultation.
- A virtual call cannot be accessed by anyone other than the patient and health care professional, unless the healthcare professional asks the patient's permission to include a third-party into the call, such as an interpreter, family member or multi-disciplinary team member.
- Patients can be seen by any healthcare professional authorised to access the Waiting Area. Authorisation is defined by a unique login and assigned roles in the platform. Organisation Administrators are responsible for assigning this access to their staff.
- There is no requirement for the patient to create an account or authenticate to use the platform. The patient's identity can be verified on the video call as would occur in a physical outpatient appointment. This information will be purged once the call is complete.
- The system will provide appropriate levels of call encryption to protect the disclosure of patient identifiable information, ensuring confidence in the system.
- Attend Anywhere has a three-tier privacy and security model (see Appendices 1 & 2).

Purpose / Objectives - Why is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project.

The purpose of the project is to pilot video clinic consultations using the video consultation software, Attend Anywhere and to evaluate the benefits to patients, staff and the trust. Embracing new consultation media is also a key feature of the NHS Long Term Plan.

Potential benefits to patients:

- More convenient, less stressful and overall a better experience
- Reduction in amount of time required to attend an appointment
- Reduction in travel costs (public transport, parking
-

Potential benefits to the trust:

- Reduction in the number of patients attending outpatients, freeing up space
- Reduction in the number of journeys, reducing carbon footprint
- Reduction in unnecessary patient transport

What is the purpose of collecting the information within the system? For example patient treatment, patient administration, research, audit, reporting, staff administration etc.

- Patients will be asked to verbally agree to participate in the video consultation pilot. When accessing the Attend Anywhere waiting area they will be asked to provide their first name, surname, date of birth and mobile number. This is required so that the patient can be identified in the waiting form but also so they contacted if there are any technical problems.

- Notifications can be sent to a clinician's phone or desktop to alert them that there is a patient in the waiting area but no patient details are included in the message.

- For staff to create an account they will need to provide their details to Attend Anywhere. This information will be used to determine individual permissions and roles in the management console in Attend Anywhere

- Any responses from the optional Survey Monkey patient experience survey that patients will be asked to complete will be anonymous and will be used to evaluate the quality of the patient's video consultation experience.

- During the consultation, healthcare professionals will obviously discuss personal and clinical information as part of the usual clinician-patient relationship

What are the potential privacy impacts of this proposal - how will this change impact upon the data subject? Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing.

Patients' privacy may be impacted if they do not use a private space when taking part in a video clinic. To mitigate this, Royal Free clinicians will advise patients to find a private space and ensure they cannot be overheard during the video appointment.

Attend Anywhere is completely confidential and secure. Patients have their own private video room that only authorised healthcare professionals can enter. They cannot see the details of other patients in the waiting area.

Provide details of any previous Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a PIA may have been undertaken during the project implementation

Not applicable

Stakeholders - who is involved in this project/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change.

The project team is working closely with clinicians and operations managers within the services that wish to pilot video consultations and also has a working group which meets fortnightly and includes stakeholders from IT, Comms, Cerner back office and the Outpatient Appointment Centre. Other stakeholders such as IG are being consulted on an "as needed" basis.
It is also planned to run a number of workshops with the trust's Equal Access patient groups that operate on each of the three main sites.

Section C - The data involved

What data is being collected, shared or used?
(If there is a chart or diagram to explain attach it as an appendix)

Data type			Justifications – there must be justification for collecting the particular items and these must be specified here – consider which data items you could remove, without compromising the needs of the project?
Information that identifies the individual and their personal characteristics	Name	☒	The data is temporarily collected to aid in the identification of patients for their appointment but is removed once they leave the waiting area.
	Address	☐	
	Postcode	☐	
	Dob	☒	
	Age	☐	
	Sex	☐	
	Gender	☐	
	Racial/ethnic origin	☐	
	Tel no.	☐	
	Physical description	☐	
	NHS no.	☐	
	Mobile/home phone no.	☒	
	Email address	☐	

Data type	Yes	N/A	Justification
Information relating to the individual's physical or mental health or condition	☒	☐	The video appointment will be a full clinician-patient consultation and will involve the patient giving information that is relevant to their condition
Information relating to the individual's sexual life	☒	☐	Only if directly relevant to the clinical consultation (no different from face-to-face)
Information relating to the family of the individual and the individuals lifestyle and social circumstances	☒	☐	If relevant as part of the clinical consultation
Information relating to any offences committed or alleged to be committed by the individual	☐	☒	
Information relating to criminal proceedings, outcomes and sentences regarding the individual	☐	☒	
Information which relates to the education and any professional training of the individual	☐	☒	
Employment and career history	☐	☒	
Information relating to the financial affairs of the individual	☐	☒	
Information relating to the individual's religion or other beliefs	☒	☐	Possibly if relevant to the patient's clinical condition and would need to be discussed as part of the consultation
Information relating to the individual's membership of a trade union	☐	☒	

Section D – Assessment questions

	Question	Response	Required Action
Legal compliance – is it fair and lawful?	1. What is the legal basis for processing the information? *This should include which conditions for processing under the Data Protection Act and GDPR apply and the common law duty of confidentiality.*	The lawful basis for processing is GDPR Art. 6 (e) "Public Task" and Art. 9 (h) processing necessary for "medical diagnosis" and "the provision of health and social care". Processing is necessary for the performance of a task carried out in the public interest, for public health purposes and for the purposes of preventative or occupational medicine	
	2. (a) - Is the processing of individual's information likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act? (b) - Have you identified the social need and aims of the initiative and are the planned actions a proportionate response to the social need?	No Yes	
	3. It is important that individuals affected by the initiative are informed as to what is happening with their information. Is this covered by fair processing information already provided to individuals or is a new or revised communication needed?	Yes	
	4. If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?	Consent will be obtained verbally and will be documented in the medical notes. If patients withdraw their consent, they will either continue the consultation by telephone or will be offered a face-to-face appointment	

Purpose	5. Does the project involve the use of existing personal data for new purposes?	Yes	
	6. Are potential new purposes likely to be identified as the scope of the project expands?	No	
Adequacy	7. Is the information you are using likely to be of good enough quality for the purposes it is used for?	Yes. It is used solely for the purpose of identifying the correct patient in the waiting area and then deleted after the consultation	
Accurate and up to date	8. Are you able to amend information when necessary to ensure it is up to date?	Not applicable	
	9. How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Patients will have to enter their own details in order to access the waiting room. Clinicians will confirm their identity when they start the consultation	Presumably there is nothing to stop them entering false details but this would mean clinicians cannot identify them
Retention	10. What are the retention periods for the personal information and how will this be implemented?	Attend Anywhere do not use, disclose or store any of the personal information that patients have provided in order to access the platform. Any personal information entered is deleted from the system following the end of the consultation and the information is only used to identify the patient in the Waiting Area	
	11. Are there any exceptional circumstances for retaining certain data for longer than the normal period?	Not applicable	
	12. How will information be fully anonymised or destroyed after it is no longer necessary?	Not applicable. The information is deleted at the end of the video appointment	
Rights of the individual	13. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held?	Not applicable as no data will be held	Details of the consultation will be documented in medical notes and clinic letters in exactly the same way as for a face-to-face clinic

Appropriate technical and organisational measures	14. What procedures are in place to ensure that all staff with access to the information have adequate information governance training?	Usual trust processes plus clinicians will not be given access unless they have completed their IG training	
	15. If you are using an electronic system to process the information, what security measures are in place?	Not applicable	
	16. How will the information be provided, collated and used?	The information will be used to identify the patient in the waiting area and then deleted after the consultation	
	17. What security measures will be used to transfer the identifiable information?	Not applicable	
Transfers both internal and external including outside of the EEA	18. Will an individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?	No	
	19. Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data?	No data will be transferred	
Consultation	20. Who should you consult to identify the privacy risks and how will you do this? Identify both internal and external stakeholders. *Link back to stakeholders on page 3.*	See stakeholder section B	
	21. Following the consultation – what privacy risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc.	See section E	
Guidance used	22. List any national guidance applicable to the initiative that is referred to.	Attend Anywhere documentation	

Section E – Privacy issues identified and risk analysis

1) Identify the privacy and related risks (see Appendix 1 for further information)

Nb. By allocating a reference number to each identified privacy issue will ensure you link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified in column

Table 1

Ref No.	**Privacy issue –** element of the initiative that gives rise to the risk	**(a) Risk to individuals** *(complete if appropriate to issue or put not applicable)*	**(b) Compliance risk** *(complete if appropriate to issue or put not applicable)*	**(c) Associated organisation/ corporate risk** *(complete if appropriate to issue or put not applicable)*
	Consultation being overheard/interrupted at clinician's end (at work)	Inappropriate identification or the disclosure of information	Non-compliance with the DPA. Non-compliance with the common law duty of confidentiality	Non-compliance with GDPR and other legislation
	Patients may not be in a private area whilst taking part in a video consultation	Inappropriate sharing of information	Non-compliance with the common law duty of confidentiality	Non-compliance with GDPR and other legislation
	Patients may take a recording of their video consultation	Not applicable	Non-compliant with trust policy if clinician is not informed	Not applicable
	A staff member may impersonate a clinician and gain access to a video waiting room	Inappropriate sharing of information	Non-compliance with the DPA	Non-compliance with GDPR and other legislation
	Insufficient spyware and virus protection on non-trust computers	Inappropriate sharing of information	Non-compliance with the PECR regulations	Non-compliance with GDPR and other legislation
	Third party accessing the history of a consultation (eg call logs on the patient device	Inappropriate sharing of information	Non-compliance with the common law duty of confidentiality Non-compliance with the DPA	Non-compliance with GDPR and other legislation
	Clinician does not read/comply with the required privacy standards	Inappropriate sharing of information	Non-compliance with the common law duty of confidentiality, with the DPA and with PECR	Non-compliance with GDPR and other legislation
	Clinician does not comply with consent requirements (ie not giving patients necessary information about risks, not recording their consent	Patient unable to give informed consent	Non-compliance with the DPA	Non-compliance with GDPR and other legislation

2) Identify the privacy solutions

Table 2

Ref No.	Risk – taken from column (a), (b) and/or (c) in table 1.	Risk score – see tables at Appendix 2			Proposed solution(s) /mitigating action(s)	**Result:** is the risk accepted, eliminated, or reduced?	Risk to individuals is now OK? Signed off by?
		Likelihood	Impact	RAG status			
1	Consultation being overheard/interrupted at clinician's end (at work)	3	3	9	Clinicians to ensure they are in a private room with a "Do Not Disturb" notice on door	Reduced	
2	Patients may not be in a private area whilst taking part in a video consultation	3	3	9	Patients will be advised by the clinician that they cannot continue with the consultation	Reduced	
3	Patients may take a recording of their video consultation	3	2	6	Patients are asked not to do this in the information leaflet	Reduced	
4	A staff member may impersonate a clinician and gain access to a video waiting room	2	4	8	Web-based system uses private video rooms for each consultation	Eliminated	
5	Insufficient spyware and virus protection on non-trust computers	4	4	16	Clinicians to sign to confirm they will only use Trust IT equipment	Reduced	
6	Third party accessing the history of a consultation (eg call logs on the patient device)	3	2	6	Clinicians to advise patients to delete browsing history if this is a concern	Reduced	
7	Clinician does not read/comply with the required privacy standards	3	4	12	Clinicians to sign to confirm they will follow the guidelines for video appointments	Reduced	
8	Clinician does not comply with consent requirements (ie not giving patients necessary information about risks, not recording their consent	3	4	12	Clinicians to sign to confirm they will follow the guidelines for video appointments	Reduced	

3) Integrate the PIA outcomes back into the project plan

NB. This must include any actions identified in Table 1 and Table 2.

Who is responsible for integrating the PIA outcomes back in to the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?							
Ref No.	**Action to be taken**	**Date for completion of actions**	**Anticipated risk score following mitigation**			**Responsibility for action – *job title not names***	**Current status/progress**
			Likelihood	**Impact**	**RAG status**		
1	Draft guidelines for all clinicians to ensure they follow confidentiality & consent requirements (to mitigate risk 1)	31/10/19	3	3	9	*Project Manager*	*Ready to pilot*
2	Draft guidelines for all clinicians to ensure they follow confidentiality & consent requirements (to mitigate risk 2)	31/10/19	3	3	9	*Project Manager*	*Ready to pilot*
3	Draft guidelines for all clinicians to ensure they follow confidentiality & consent requirements (to mitigate risk 5)	31/10/19	4	4	16	*Project Manager*	*Ready to pilot*
4	Draft guidelines for all clinicians to ensure they follow confidentiality & consent requirements (to mitigate risk 7)	31/10/19	3	4	12	*Project Manager*	*Ready to pilot*
5	Draft guidelines for all clinicians to ensure they follow confidentiality & consent requirements (to mitigate risk 8)	31/10/19	3	4	12	*Project Manager*	*Ready to pilot*
6	Include guidance on risk 3 in Patient Information leaflet & clinician guidelines	31/10/19	3	2	6	*Project Manager*	*Ready to pilot*
7	Include guidance on risk 6 in practical guidelines for clinicians	31/10/19	3	2	6	*Project Manager*	*Ready to pilot*
8	Include confirmation of IG training & guidelines as part of sign-off process for any clinicians starting to use the platform	31/10/19	2	2	4	*Project Manager*	*Ready to pilot*

Section F - Data Protection Impact Assessment – review and sign off

If you identify a high risk and you cannot mitigate that risk, the trust must consult the ICO before starting the processing*. Please add details below.

* only required post 25 May 2018 implementation of GDPR

RFL Data Protection Officer (name)	[redacted]
Signature	[redacted]
Date of DPIA sign off	17 October 2019
Date of DPIA review	

Copy to be retained by project manager and also IG team.

Appendix 1: Types of privacy risk

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Compliance risk

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015
- Non-compliance with the DPA.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Associated organisation/corporate risk

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Appendix 2: Guidance for completing a risk register

- What is the actual risk? Make sure the risk is clear and concise and articulated with appropriate use of language, suitable for the public domain.
- Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests
- Don't reference blame to other organisations in the risk register (the register may be made available in the public domain)
- Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

Likelihood

	Score				
Likelihood score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency - how often might it happen?	This probably will never happen/recur	Do not expect it to happen/recur, but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur, but is not a persisting issue or circumstance	Almost certain to happen/recur; possibly frequently

Impact

	Score				
Impact score	1	2	3	4	5
Descriptor	Very low	Low	Medium	High	Very high
Impact should it happen?	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probable it will have a significant impact	Will have a major impact

Using the risk "RAG" rating system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

Impact	Very High -5	A	A/R	R	R	R
	High - 4	A	A	A/R	R	R
	Medium - 3	A/G	A	A	A/R	A/R
	Low - 2	G	A/G	A/G	A	A
	Very Low - 1	G	G	G	G	G
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		Likelihood				

Version Control Sheet

Version	Date	Author	Status	Comment
1.0	24/07/2018	IG manager, Data Protection Officer	Previous version	New, approved at the IG group
1.1	17/07/2019	IG manager	Live	Minor amendments, typos formatting etc