NAViGO Digital Healthcare Projects Data Protection Impact Assessment (GDPR DPIA)

Zoom virtual meeting application during Covid19

Adapted from CPG version adapted from IG Alliance Guidance http://systems.hscic.gov.uk/infogov/iga/

Privacy Impact Assessments

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 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 data protection impact assessment(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.

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)
- 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).

The patient / Service User Perspective

It helps an organisation to see things from the patient's point of view. It is their data that is being used and 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.

Where do you start?

A lead person should be nominated to co-ordinate the DPIA process.

A DPIA starts with a screening process. The screening questions are provided in the table on the next page. 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.

If you answer "yes" or "unsure" to any of the screening questions in the table, you will need to undertake the DPIA. You may find it helpful to seek assistance from an information governance expert to help you with the process.

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. Remember! – imagine this initiative involved the use of your own information or that of a relative

		Yes	No	Unsure	Comments
i	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?	☒	☐	☐	
ii	Will the initiative involve the collection of new information about individuals?	☐	☒	☐	No, an invitation to a Zoom consultation should be sent to the patients preferred method of communication already recorded in SystmOne. For internal meetings, staff will authenticate using existing NHS email address information.
iii	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☒	☐	☐	Need to use applications to contact SU's remotely due to Covid19 precautions in place, replacing face to face consultations.
iv	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?	☒	☐	☐	Directly into their homes/private environment via electronic communications
v	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☒	☐	☐	It is not necessary as part of the consultation process for any disclosure by NAViGO to Zoom or other organisations. However personal information such as email and IP address will be collected by Zoom when a contact is established. Please see DPA agreement and PN.

[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

vi	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?	☐	☒	☐	Use of virtual communications could be new technology for some persons. No facial recognition or biometrics.
vii	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐	☒	☐	

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 Data protection impact assessment as it will not apply to the 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 DPIA

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

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.

Does my project need a DPIA?

Whilst a DPIA is not a legal requirement the ICO may often ask an organisation whether they have carried out a DPIA. If your project is new, or you are planning changes to an existing system, then the time is right for conducting a DPIA. 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 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

Data protection impact assessment Template

Section 1: Background Information

Project Name Zoom - application for use to conduct business meetings and with Service Users.	
Organisation	NAViGO CIC
Assessment Completed By	Lisa Denton
Job Title	
Date completed	
Phone	
E-mail:	

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.

Use of Zoom video conferencing software for use in business planning and to contact Service Users during the Covid19 pandemic.

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.

Whilst persons are working remotely it is still necessary to conduct business meetings and contact service users. This application will allow this to be done remotely thereby limiting contact.

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

The main purpose will be to conduct business meetings for planning but there may be a need to contact and advise service users using this method. This could include advice to service users on treatment.

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.

Whilst all service user data is held securely on NAViGO systems contact via Zoom may be necessary in order to collect information to update existing records. This could mean that PD of SU's could be held on the Zoom system including email, log in, name and IP address. This is deemed necessary in the current situation in order to deliver essential services where possible. Information will not be recorded and persons will be informed that their limited PD will be collected in this way via access to the Zoom PN.

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

This is a new DPIA as this type of communication app has not been used before.

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.

NAViGO staff and service users, please list all here.

Section 2: 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	☒	**This will be necessary to contact individuals.**
	Address	☐	
	Postcode	☐	
	Dob	☐	
	Age	☐	
	Sex	☐	
	Gender	☐	
	Racial/ethnic origin	☐	
	Tel no.	☐	
	Physical description	☐	
	NHS no.	☐	
	Mobile/home phone no.	☒	
	Email address	☒	

	Y	N/A	Justification
Information relating to the individual's physical or mental health or condition	☒	☐	**Part of SU information**
Information relating to the individual's sexual life	☒	☐	**Information of SU's will be transmitted across the secure Zoom network for the purposes of communication but will not be stored by Zoom.**
Information relating to the family of the individual and the individuals lifestyle and social circumstances	☒	☐	**Information of SU's will be transmitted across the secure Zoom network for the purposes of communication but will not be stored by Zoom.**
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	☒	☐	**Information of SU's will be transmitted across the secure Zoom network for the purposes of communication but will not be stored by Zoom.**
Employment and career history	☒	☐	**Information of SU's will be transmitted across the secure Zoom network for the purposes of communication but will not be stored by Zoom.**

Information relating to the financial affairs of the individual	☒	☐	**Information of SU's will be transmitted across the secure Zoom network for the purposes of communication but will not be stored by Zoom.**
Information relating to the individual's religion or other beliefs	☒	☐	**Information of SU's will be transmitted across the secure Zoom network for the purposes of communication but will not be stored by Zoom.**
Information relating to the individual's membership of a trade union	☐	☐	

Section 3: Assessment

	Question	Response	Required Action E.g. Seek Information Governance advice
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 2018 and the common law duty of confidentiality.*	**Art 6(1)(e) public task and 9(2)(h) - helath and scosial care and Sched 1 part 1 para 1(2) DPA 2018 for service users.**	
	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 - planning for contact with SU's in time of emergency.**	
	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?	**There is a PN on the zoom website that individuals will be directed to.** **Will update main NAViGO PN with a statement regarding alternative methods of communication during this time.**	
	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	**Consent will be obtained verbally by the member of staff engaging with the SU and recorded on their NAViGO file in order**	**Standard text to be produced and approved by Corporate Governance Committee to support the Service Users awareness of any privacy and consent**

	you do if permission is withheld or given but later withdrawn?	**to demonstrate compliance.**	**requirements to be added to all invitations for a video consultation.**
Purpose	5. Does the project involve the use of existing personal data for new purposes?	**No - just a new method of communication. Collection and purpose have not changed.**	
	6. Are potential new purposes likely to be identified as the scope of the project expands?	**Unknown**	

Adequacy	7. Is the information you are using likely to be of good enough quality for the purposes it is used for?	Yes - Zoom app allows remote face to face contact with SU's and staff where necessary.	
Accurate and up to date	8. Are you able to amend information when necessary to ensure it is up to date?	**Yes**	
	9. How are you ensuring that personal data obtained from individuals or other organisations is accurate?	**Face to face contact**	
Retention	10. What are the retention periods for the personal information and how will this be implemented?	**Unchanged. Calls-video conferences will not be recorded.**	
	11. Are there any exceptional circumstances for retaining certain data for longer than the normal period?	**No**	
	12. How will information be fully anonymised or destroyed after it is no longer necessary?	**Data not stored**	
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?	**Usual subject access rights remain unchanged for information on NAViGO systems. Nothing will be stored on Zoom.**	

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 DPA training in place. Instructions will be given to staff using the Zoom app to ensure security**	
	15. If you are using an electronic system to process the information, what security measures are in place?	**N/A**	
	16. How will the information be provided, collated and used?	N/A	
	17. What security measures will be used to transfer the identifiable information?	N/A	
Transfers both internal and external including outside of the EEA	18. Will individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?	Only name email and IP and ISP information will be disclosed to Zoom	
	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?	Yes - app is managed from USA with GDPR terms in place for UK users.	
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.*	**DPO/F4IT /SIRO/Caldicott Guardian. Navigo Corporate Governance Committee. Technical experts in the Performance & Assurance Team**	**Peer review of the risks and development of the completed DPIA.**
	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.	**No more physical intrusion into people's homes than with a personal visit. Some minimal collection of PD by Zoom application**	

Section 3 – Privacy issues identified and risk analysis

a) 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)*
1	**Sharing of PD with Zoom application**	**Prospect of 'Hacking' or unlawful access whilst using the app**	**Breach of principle 6 - security**	**As (b)**

NHS Information Governance advice is here relating to Covid19:

https://www.nhsx.nhs.uk/key-information-and-tools/information-governance-guidance

b) 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	Unauthorised access whilst using Zoom app	3	3	A	Comply with all security requirements for using Zoom. Inform SU's. Lock meetings.	Accepted	DPO

c) Integrate the DPIA 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 DPIA 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	**Comply with all recommended security settings. Do not record meetings**	**Before go live**	**2**	**2**	**G**	**Lead officer**	**In progress**

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?

CPG uses 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 Consequence score. Each risk will be RAG rated by taking the Likelihood and Consequence scores, and using the matrix below:

Likelihood

1	**Rare**	**Only occurs in exceptional circumstances, <1%, 1 – 5 year strategic risk**
2	**Unlikely**	**Could occur at some time, 1- 5%, at least annually**
3	**Possible**	**Should occur at some time, 6 – 20%, at least monthly**
4	**Likely**	**Will probably occur, 21 – 50%, at least weekly**
5	**Almost Certain**	**Expected to occur, > 50%, at least daily**

Consequence

Choose the most appropriate domain for the identified risk from the left hand side of the table then work along the columns in same row to assess the severity of the risk on the scale of 1 to 5 to determine the consequence score, which is the number given at the top of the column.

	Impact (Consequence) score and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients

Quality/complaints/audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards
Human resources/ organisational development/staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage –long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business objectives/ projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met

Finance including claims	Small loss Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service/business interruption Environmental impact	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Risk Score

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.

Likelihood	**Consequence**				
	1 Insignificant	**2 Minor**	**3 Moderate**	**4 Major**	**5 Catastrophic**
5 - Almost Certain	Low Risk	Medium Risk	Medium Risk	High Risk	High Risk
4 - Likely	Low Risk	Medium Risk	Medium Risk	High Risk	High Risk
3 - Possible	Low Risk	Low Risk	Medium Risk	Medium Risk	Medium Risk
2 - Unlikely	Low Risk	Low Risk	Low Risk	Medium Risk	Medium Risk
1 - Rare	Low Risk	Low Risk	Low Risk	Low Risk	Low Risk