NHS
Bedfordshire Hospitals
NHS Foundation Trust

Data Protection Impact Assessment (DPIA) and Action Plan – For Implementation of New/Updated Systems or Processes

As a Data Controller the Trust is legally required to conduct a DPIA where the *processing of **personal identifiable data (PID) or ***sensitive data could result in risks to the rights and freedoms of the individuals whose data is being processed (this includes their right to confidentiality).

Please answer the screening questions and if the project does not involve the collection, recording, storing or processing of personal-confidential/business-sensitive data which results in all answers stated as **'NO'** a Data Protection Impact Assessment is not required and should be documented in the project or business case.

Where you answer **'YES'** to any of screening questions a DPIA **MUST** be completed as the Trust is required by law to protect information through the implementation and use of appropriate technical and organisational measures to protect PID from:

- Unauthorised or unlawful processing,
- Inappropriate access
- Inappropriate sharing or disclosure
- Accidental loss, theft, destruction, or damage.

*Processing	Defined as viewing, transferring, obtaining, using, collating and storing.
** Personal identifiable data (PID)	Data that could be used to identify an individual e.g. name, address, date of birth, NHS Number, pseudonymised data or information that could be used with other information to identify an individual including images and recordings.
*** Sensitive data	includes health information, mental capacity, ethnicity, sexuality, religious belief, biometrics

It is the responsibility of the Project Lead to ensure all actions identified during the DPIA process are completed.

Version 1.0 – June 2020

Name of Project/System/Process:	**MS Teams Patient Group Video Consultations - Trustwide**				
Version & Date:	**05/02/2021 – Version 1**				
	Name:	**Department:**	**Job title:**	**Email**	**Tel:**
Executive Sponsor:	[redacted]	[redacted]	[redacted]	[redacted]	Click or tap here to enter text.
Information Asset Owner/Administrator	[redacted]	[redacted]	[redacted]	[redacted]	Click or tap here to enter text.
Project Lead:	[redacted]	[redacted]	[redacted]	[redacted]	Click or tap here to enter text.
Person/s performing the DPIA:	[redacted]	[redacted]	[redacted]	[redacted]	Click or tap here to enter text.
	[redacted]	[redacted]	[redacted]	[redacted]	Click or tap here to enter text.
	[redacted]	[redacted]	[redacted]	[redacted]	Click or tap here to enter text.
	[redacted]	[redacted]	[redacted]	[redacted]	Click or tap here to

			Manager		enter text.

Planned start date of project/process:	04/02/2021
Planned completion date of project/process:	28/02/2021

STEP 1 - DATA PROTECTION PRIVACY IMPACT ASSESSMENT – SCREENING QUESTIONS			
Screening Questions	**Answers: YES/NO**	**Comments (Please detail response if 'Yes' selected**	**Example**
Will the project/system/device or process involve the use of patient/staff information	Yes	1. Data needed to enable staff to login (clinicians and admin staff). User details added to MS Teams to enable user to have access (Name & NHS.net email address) 2. Data that will be managed by people using it. i.e. user uploads PID (patient names) to MS teams and shared with colleagues. The only patient identifiable information to be shared will be the name of the Patient which the patient will input at the point of entering the meeting. This is the same as for a face to face meeting 3. Patient name who is accessing the group consultation	Staff member logs on to MS Teams and onto teams link for a specified group patient meeting that they are facilitating or being involved in Patients attending the group session individually also join by clicking on a unique meeting-specific link. All users, staff and patients, input their names to enable communication between participants during the meeting and to ensure that only invited patient participants are in the meeting
Will the information used be identifiable?	No	Information shared at the group session would be generic and generalised eg. health plans or examples of the kind of exercise people can do at home. No individual patient information will be shared by staff or asked for. Patients who	Could include but not conclusive: Name, Demographics, Use of identifers such as DOB, Post Code, Gender, Condition, IP Addresses

STEP 1 - DATA PROTECTION PRIVACY IMPACT ASSESSMENT – SCREENING QUESTIONS			
Screening Questions	**Answers: YES/NO**	**Comments (Please detail response if 'Yes' selected**	**Example**
		divulge personal information will do so voluntarily unprompted if they wish but no-one will be required to do so nor will it be necessary	
Is the project/system/device or process in use and being upgraded/amended?	No	But likely to have software upgrades, process changes in future	
Has a Data Protection Impact Assessment been completed previously for the project/system/device/process	Yes	MS Teams has been approved for use by the Trust however this is additional functionality to enable the Trust to use the application for patient group consultations. MS Teams has already been approved for group use for the Therapies teams.	
Will the project/system/device/process require you to evaluate or score individuals information?	No		
Will there automated decision-making undertaken without any human involvement at all	No		

STEP 1 - DATA PROTECTION PRIVACY IMPACT ASSESSMENT – SCREENING QUESTIONS			
Screening Questions	**Answers: YES/NO**	**Comments (Please detail response if 'Yes' selected**	**Example**
Will the information that you plan to use be sensitive data or data that could be assessed as including information of a highly personal nature	No		
Will the project/system/device or process involve a large number of individuals?	Yes	The platform is being made available for all employees of Bedfordshire Hospitals NHS Trust and for this particular project will be used for patient group consults. For example on average the Therapies team at Bedford Hospital are expecting approximately 1200 patients per annum – many of the consultations involve the same patients attending a course of treatment eg/ 15 dietetics patients per week attending a 9 week course on eating healthy. This would be replicated across other services running group sessions on both sites	

STEP 1 - DATA PROTECTION PRIVACY IMPACT ASSESSMENT – SCREENING QUESTIONS

Screening Questions	**Answers: YES/NO**	**Comments (Please detail response if 'Yes' selected**	**Example**
Will the project/system/device or process including data concerning vulnerable individuals or individuals with protected characteristics as defined within the Equality Act	Yes	Yes although clinical staff will assess suitability of patients to attend via MS Teams. Group sessions may be run from seminar rooms so that patients who are unable to access the virtual session because of a lack of a device or they do not feel confident using it or do not feel safe in their home can still attend in person. Or they may run separate virtual and face to face group sessions.	This could be individuals with specific needs such as the elderly, learning difficulties or children
Does your project/system/device or process plan to use innovative technological or organisational solutions	No	N/A	An example of this type of project could fall within the following:- Artificial intelligence Machine learning deep learning
Will the project/system/device or process involve activity which could prevent individuals from exercising a right or using a service or contract	No	N/A	This could apply where a research project could make a S251 application where consent is not being sought by the patient to participate
Does your project/system/device or process involve the use of Biometrics data	No	No fingerprints or facial recognition software will be used	An example of this is a project where you plan to use facial recognition or the using fingerprints to uniquely identify a person

STEP 1 - DATA PROTECTION PRIVACY IMPACT ASSESSMENT – SCREENING QUESTIONS

Screening Questions	**Answers: YES/NO**	**Comments (Please detail response if 'Yes' selected**	**Example**
Will the project/system/device or process involve the collection or use of genetic data beyond healthcare purposes	No	N/A	This genetic data could include medical diagnosis or to be used for medical research
Will the project/system/device or process be combining, comparing or matching personal data obtained from multiple sources?	Yes	Patients will be sent an email link to a phone number or email address that they have provided if the patient has consented to attend a virtual group consultation and will need to input this name to join the call – confirmed at the start of the call. They will only be able to join the call after being admitted from the lobby. The staff running the group will check that the attendees match the patients that they are expecting	In health this could be for the purpose of fraud, uptake of health services or monitoring purposes
Will the project/system/device or process use Invisible processing as a basis	No	N/A	This could be a Research study where it uses data shared from another source about individuals that hasn't been obtained from the individual directly

STEP 1 - DATA PROTECTION PRIVACY IMPACT ASSESSMENT – SCREENING QUESTIONS

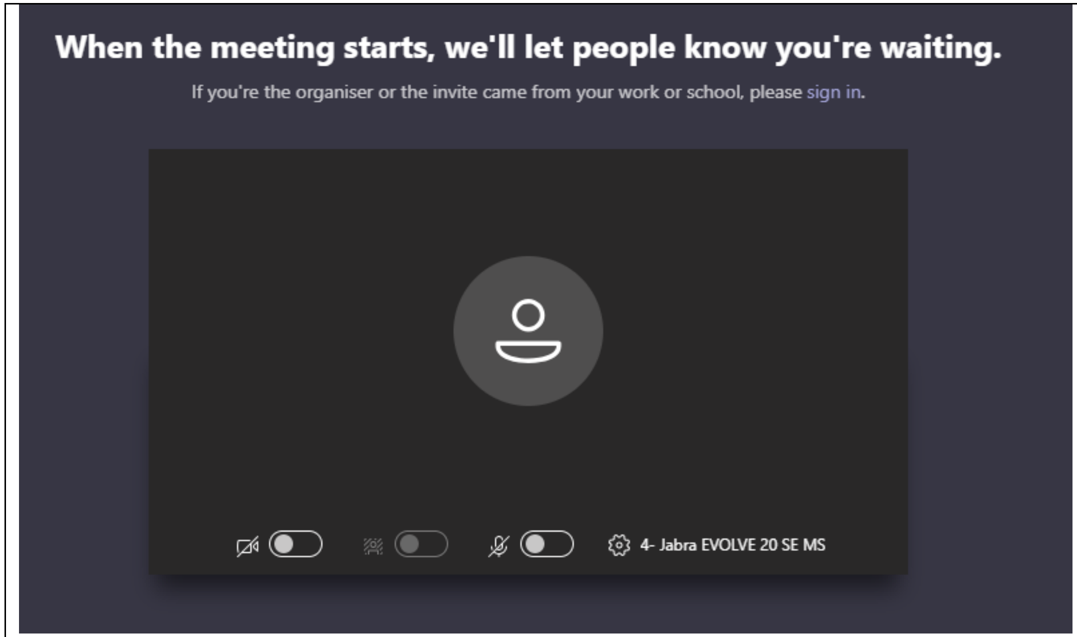
Screening Questions	**Answers: YES/NO**	**Comments (Please detail response if 'Yes' selected**	**Example**
Will the project/system/device or process be processing data which involves tracking an individual's location or behaviour	No	N/A	This could include a number of the following processes:- Fitness/lifestyle/health monitoring Data Processing in the workplace/home/remote working Wealth Profiling Use of Cookies
Is there a Risk of physical harm that could occur as a result of the project/system/process where a data breach could jeopardise the (physical) health or safety of individuals	No	Identifiable medical information is not being shared via the group consults. The Trust has already completed and approved the DPIA for the use of MS Teams and no IT security concerns identified.	This could include the following:- Loss of medical records Sensitive data being shared with a third party Use of removable media containing personal data

DPIA template

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. **The final outcomes should be integrated back into your project plan.**

Step 2: Project/System/Device or Process Information

Please provide details of the project/system/device or process *delete as appropriate:
In March 2020 access to Microsoft Teams was bought forward for NHS organisations to support remote working in response to the 'COVID-19' outbreak, in addition to Microsoft 'OneDrive' and 'Office Online' applications.which became available to all NHS mail users from 25/03/2020 free of charge. In relation to the use of NHS Mails and Office365 tools which include MS Teams the Trust is a joint data controller with NHS Digital. NHS Digital is a Joint Data Controller because of its role as the national host organisation for managing commercial relations, funding, technical and service governance and roll out and the Trust will act as a controller for data generated by staff through the use of MS Teams. A separate DPIA has been created for the overall use of teams – this document is aimed specifically at the use of the platform for group consultations. The key groups that intend to use this functionality initially were the Diabetes, Physiotherapist and Dietetics therapies at Bedford Hospital but more teams across both sites are likely to use it, eg. Luton Therapies, Bariatrics pre-surgery education group sessions, Diabetes teams, possibly hip and knee school orthopaedic group sessions etc. Patients will be sent an Outlook invite using MS Teams – they will be able to connect using their browser or MS Teams application on their mobile device. They will not be required to have an MS Teams login account. Clicking on the link sent by the meeting organiser will direct them to the chat window where they will need to join by entering their name. The patient will only have guest privileges thus will have to wait in the lobby until they are admitted in by the organiser as shown below. The recording functionality is disabled for all guest users. Attend Anywhere Video consultations platform was assessed for suitability however currently attendance is limited to a small number of people per consult and MS Teams offers the functionality to invite larger groups. If this changes, or a different provider becomes available, we will review which platform we use in the future for group sessions.



When the meeting starts, we'll let people know you're waiting.

If you're the organiser or the invite came from your work or school, please sign in.

This will be the only information that the patient will need to provide as part of this process. The meeting organiser will need to ensure that patient information is protected at all times – this includes the meeting invite NOT containing the email addresses or any additional contact information of other patients attending the Group Consultation. Therapies staff organisers will be using SystmOne which records patient email addresses. For other non-SystmOne clinics the staff organising will obtain patient email addresses where these are not routinely available on PAS (which they are currently not).

Prior to the Covid 19 outbreak and video functionality, specialities and Trust staff were carrying out patient group education sessions or focus/user groups face to face – thus the patient will have already consented to being in this group setting; however as the virtual environment will be a little different – we will do the following:

The only information which will be required and visible to other patients is the ‘ First Name’ – any other information such as age/vulnerability will be considered at an earlier stage when the patient is first offered a group setting. The intention is to remind patients at the start of the session to be vigilant of the information that is being shared. For example Bedford Hospital Diabetes has confirmed that during the sessions patients may give a summary of their condition and any applicable history; but this will be done with prior permission of the patient similar to the face to face sessions. So there will generally be no additional personal information shared that is not already shared as part of a face to face group session.

Benefits of the project/system/device or process to the Trust	
What are the benefits to the Trust and the individuals whose data will be processed?	The primary benefit of introducing this application is to allow group clinical care, education or patient focus or user groups to be offered in a virtual setting without the need for patients to attend the hospital in person. This will be more convenient for some patients and especially if they had to travel a long way (eg. Some bariatrics patients) and also contributes to the "green" strategy and sustainability, reducing the pressure on car parking spaces and car parking costs, travel time saved and reduced carbon emissions. No-one will be forced to participate in this way eg. if they do not have access to a suitable device, private space or do not feel confident to do so.
what do you want to achieve?	The hope is that specialities which previously offered 'group' sessions 'face to face' will now have the option to offer a similar service to patients virtually during Covid but also beyond.
What is the intended effect on individuals?	Patients will have access to required care similar to the same standard they were receiving prior to Covid 19 and in a more convenient way.

Purpose of project/system/device or process	
What is the purpose of the project/system/device or process e.g. Includes but not limited to Direct Care or Research	The intention of this project is to allow the hospital to offer the same levels of care to the patient virtually as face to face, where it is clinically appropriate, for example group clinical education sessions, or enable other patient groups to be offered virtually, for example focus groups or patient user groups. Where MS Teams is unsuitable for the patient either due to learning difficulties/disabilities or the patient has no technical means to attend virtually, patients will be offered a one to one telephone conversation or face to face if that is deemed more appropriate.

	Any patient contact should be documented in the same way that it would have been for face to face contacts.

Will there be sharing of data with anyone such as a supplier/third party/NHS Partner or internally between systems (this can include maintenance and support from a supplier), please detail. What level of data is to be shared – Level 0, 1, 2, 3, 4 (Please supply Third party supplier screening document and Third Party Supplier Security Questionnaire if relevant and 'Schedule of Processing' if contract already signed)
Accenture is the processor for NHS Mail and O365 applications with Microsoft as a sub processor

How will the information be stored (Pull Down Menu)	**Where will the information be stored?**
Cloud	Within the UK

Does the supplier use sub-processor(s) to provide the service/support to the Trust?	
Yes (Please detail below)	
Service being provided by sub-processor(s)	**Where is information stored (please detail country)**
Microsoft Office Applications	**Exchange Online via a cloud based NHS tenant of Office 365**

Where PID is transferred, stored or viewed outside of the UK, please provide details of the purposes below.
Not applicable as this functionality has been disabled by NHS Digital as part of the rollout.

Please include a data flow map images that documents the technical architecture to include how the system interfaces with other Trust systems and the external supplier. The data flow diagram should also include the sharing of data with the supplier and relevant outputs e.g. letter generated to patient along with any security related controls such as encryption at each stage of the data flow.
Technical Architecture Diagram [redacted]
Data Flow Diagram

[redacted]

Please detail below each data categories being processed by purpose and type								
Category	Who's Information	System	Where is it going?	Nature and purpose of the processing	Frequency (e.g. daily, weekly, monthly, real time)	Method of Transport	PID/No PID	Type of Information
Identification of patients to attend virtual group consultations	Patient name	MS Teams	Stored within NHSmail in the UK and USA. May be viewed outside of the EU.	Administration of services provided by NHSmail	Real-time	Electronic system transfer - EST	PID	➢ Method to achieve consent will be a mix of calling the patient and obtaining the consent at an initial consultation ➢ Consent information will be stored on SystemOne, Trust internal drive or locked files. ➢ Invites shared from a shared inbox or link to meeting sent via text if that's the preferred method of contact.
Patient contacted	Employee/ Patient	iPM	May be stored within iPM	Patient contact may be logged on iPM	Real time	Manual	PID	Type of contact made and the purpose

ACCESS CONTROL: Who will have access to the PID, why do they need access, how will they access it, what will they have access to, when will they need access to it, and how will access be controlled? This may be through direct access to an IT system or through sharing of the PID by other means E.g. reports emailed etc.				
Please list Who,	**Why?**	**When?**	**How?**	**What?**
Bedfordshire Hospitals employees	Collaboration purposes	Ongoing	Each employee requiring access will have an NHS.net account and will be able to access Teams remotely. Patients are invited as guest users and will not have access to any other confidential information.	Invites will be sent out by the administration team of each department from shared or individual hospital mail boxes.

Step 3: Describe the scope of processing

Describe the scope of the processing: what is the nature of the data, and does it include special (sensitive data) category or criminal offence data? How much data will you be collecting and using (pseudonymised/identifiable information? How often? How long will you keep it? How many individuals are affected?	
What is the nature of the data? E.g. patient medical information, diagnosis, procedure, employee information, IP Addresses images (such as x-ray, MRI, CCTV)	As part of Group Consultations- the meeting organizers will need to ensure patient identifiable information is not being shared on the platform.
Does the data include special (sensitive data) category or criminal offence data?	It is likely that data uploaded into Ms Teams will include patient identifiable information and will include special category data however as part of Group Consultations the use of any patient identifiable information apart from the Name will not be needed as will be strongly discouraged.
How much data will be collected? (volume/unique patients)	No data will be collected on MS Teams
Is the project/system/device or process intending to use identifiable or pseudonymised information?	Patients will be the direct consumer of the service – they will be accessing the link to the session using their name only.
How often is the information collected e.g. real time, daily, weekly, monthly, quarterly, annual	Information is updated within MS Teams in real-time
How long will the information be kept for?	No data will be collected
Will any of the information be shared routinely with any other NHS Partners (e.g. CCG, Care Providers, NHS Organisations0	Yes if partners have an nhs.net account although this process is specifically for virtual patient group consultations only.
Could the information collected be used for any purposes beyond the primary purpose as defined in Step 1 e.g. research/teaching	This is unlikely however if any information is collected within MS Teams and could be used for the purpose beyond what was intended then consent and research

purposes	governance processes would apply
Will a test environment be required as part of the deployment e.g. will it include live/dummy patients	Local testing will be undertaken by the IT Projects team prior to roll out and will not include any patient data. The use of MS Teams for group consultations is already in use for the therapies teams.
Is there a training requirement for staff as part of the deployment process. How will this be achieved?	Training guides are available on NHS Mail. An SOP has been developed for staff use in delivering virtual group patient sessions.

Describe the context of the processing: How much control will an individual have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in?		
what is the nature of your relationship with the individuals (clinical/non-clinical/corporate)?	Clinical group consultations by Clinical Nurse Specialists, Therapists, Doctors or other clinicians, or could be with non-clinical staff for things such as patient experience user groups or focus groups	
Would individuals expect you to use their data in this way?	The Trust is not processing any data held in MS Teams in a novel way.	
Where it has been identified within the checklist that the group will include children, vulnerable groups (learning difficulties/disabilities, hearing/sight impaired). Please describe how the processing may affect this group and attach the Quality Impact Assessment Screening Form to the documentation to detail positive/negative effect	☐ Not Applicable	
	☒ Children	Where this application is used with children we would expect it will be used with their parents/guardians present
	☒ Vulnerable adults	Any vulnerable patients will be offered one to one virtual sessions with carers present if required or telephone advice or referred back to surgery as not suitable until face to face can restart safely, or face to face beyond Covid. Other Services – Patients will be

		assessed for vulnerabilities and if identified as not suitable for Group Consultations they will be offered a 1-2-1 virtually or face to face.
	☒ Safeguarding Adults/Children	As above If identified, will not be offered Group Consultations for any service but rather a 1-2-1 consultation.
	☒ Hearing/Sight Impaired	This application would only be used for hearing/sight impaired if they confirmed that they would have someone available to help them, eg. carer, and that this would not be detrimental. It may be no more or less detrimental than a face to face group session. It would be fair to give them the choice.
Where it has been identified within the screening checklist that it will include patients with protected characteristics, please select which group this could affect and also attach the Quality Impact Assessment Screening Form to the documentation to detail positive/negative effects	☐ Not Applicable ☒ Age ☒ Disability ☒ Gender Reassignment ☒ Marriage/Civil Partnership ☒ Pregnancy/Maternity ☒ Race ☒ Religion or belief ☒ Sex ☒ Sexual Orientation See separate Equality Impact Assessment for video consultations	
Does the Trust's privacy notice (staff/patients) detail the purpose as outlined in this DPIA	Not applicable	

Are there any issues of public concern that you should factor in e.g. would the public expect the Trust their information to be used in this way. This could include the use of AI, tracking, profiling.	Not applicable	
Does system comply with the Individual Rights of Individuals?	☒the right to be informed	Individual permission will be sought from the patients to participate in the consultation.
	☒ The Right of Access	Individual permission will be sought from the patients to participate in the consultation. Usual request process applies
	☒ The Right to Rectification	No PID apart from the patient name will be stored – the patient is able to update his/her name when attending group consult. Normal Trust process applies to rectify information.
	☒ Right to Erasure or Restrict Processing	As per Trust policies.
	☒ Right not to be subject to Automated Decision Making	Individual permission will be sought from the patients to participate in the consultation.
Compliance with Statutory requirements	☐ Data Quality/Clinical Coding requirements	[Please describe how]
	☐ Is there functionality for records to be redacted if applicable (medico-legal or subject access purposes)	N/A. Local Trust policies apply if any documentation is to be redacted.
	☐ If an IT system does it comply with the requirement for adoption/transgender records to be masked and a new identity	N/A

	created.	
	☐ Does processing comply with the NHS Records Management Code of Practice 2016 relation to retention/destruction requirements	Yes, the Trust adheres to the national policy in relation to retention/destruction of documents.
	If an IT system does it allow for the patients to set preferences for contact (e.g. receiving communications by email, post)	N/A

Please indicate below what data will be processed as part of this project: Individual's information MUST NOT be processed "just in case it is needed", it MUST be limited to what IS required to achieve the intended purpose.		
Data Items	**Yes or No** Purpose	**Purpose**
Name	**Yes**	The patient will be invited to the 'Group session' as a guest and will only be admitted by the meeting organiser who will be a member of the Trust. The name is the only identifier that will be required – all other information related to NHSmail users is covered in the central 'teams' DPIA.
Address	**No**	[Please describe purpose]
Part Postcode only e.g. LU4, MK45	**No**	[Please describe purpose]
Full postcode e.g. LU4 0DZ	**No**	[Please describe purpose]
Date of birth	**No**	[Please describe purpose]
e-mail address	**No**	[Please describe purpose]
Telephone Numbers	**No**	[Please describe purpose]
Mobile Number	**No**	[Please describe purpose]
Gender	**No**	[Please describe purpose]
Marital Status/Civil Partnership	**No**	[Please describe purpose]
Next of Kin	**No**	[Please describe purpose]
NHS Number	**No**	[Please describe purpose]

Please indicate below what data will be processed as part of this project: Individual’s information MUST NOT be processed “just in case it is needed”, it MUST be limited to what IS required to achieve the intended purpose.		
Hospital Number	**No**	[Please describe purpose]
Payroll Number	**No**	[Please describe purpose]
Bank Details	**No**	[Please describe purpose]
Bank/Payment Card details	**No**	[Please describe purpose]
Health information	**No**	[Please describe purpose]
Occupational Health information	**No**	[Please describe purpose]
Sexual Orientation	**No**	[Please describe purpose]
Ethnicity	**No**	[Please describe purpose]
Political Interest	**No**	[Please describe purpose]
Union Membership	**No**	[Please describe purpose]
Religious belief	**No**	[Please describe purpose]
Safeguarding Information	**No**	[Please describe purpose]
Visual/Hearing Impairment	**No**	[Please describe purpose]
Frequency identifier tags (RFID)	**No**	[Please describe purpose]
IP addresses	**No**	[Please describe purpose]
Wi-Fi tracking	**No**	[Please describe purpose]
Number plate Recognition	**No**	[Please describe purpose]
Video Recordings	**No**	[Please describe purpose]
Voice Recordings	**No**	[Please describe purpose]
CCTV	**No**	[Please describe purpose]
Identifiable photographs	**No**	[Please describe purpose]
Non identifiable photographs	**No**	[Please describe purpose]
Identifiable clinical images e.g. x-rays, MRIs	**No**	[Please describe purpose]
Non identifiable clinical images e.g. x-rays, MRIs	**No**	[Please describe purpose]
DNA	**No**	[Please describe purpose]

Step 4: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
IG Team – to ensure all IG aspects have been considered and addressed so Group Consultations in all Trust services can take place. IT Team – are supporting and advising in how to set this up securely and confidentially Bedford Therapies team – who have already used this within their service with patients successfully Other specialties who have requested this group patient session functionality

Step 5: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing (please see Appendix 4 for description)? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep (used for purposes beyond what was originally intended)? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their individual rights? What measures do you take to ensure processors/third parties comply? How do you safeguard any international transfers?

Principle 1 - Personal Data shall be processed fairly and lawfully	Please specify the lawful basis for processing:- Article 6 (e); - Public task - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller *Article 9 (2) (h) – processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*
Principle 2 – Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed	No information uploaded into MS Teams will be further processed beyond the purpose it was originally obtained for.
Principle 3 – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed	Users of MS Teams and 'Team Managers' will be responsible for ensuring information stored within the software is relevant and not excessive. Only patients name will be used which is entered by patient themselves.

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.	'Teams Managers' will be responsible for ensuring data stored is up to date and will be responsible for removing members no longer applicable to that team. Line managers for NHSMail users who leave the Trust will be responsible for ensuring that Trust data is retrieved prior to leaving the organisation.
Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	The Records Management Code of Practice applies to files uploaded into Teams and individuals will adhere to this Code as is normal practice or is required by law. NHS Mail holds audit trail information for 180 days from the last point of access.
Principle 6 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	The NHSmail Live Service is accredited to the NHS secure email standard and is compliant with ISO27001 and a number of security standards. As users the Trust is required to complete an annual Data Security & Protection toolkit. The Trust has appointed a Local Administrator (IT Service Desk) to manage and maintain the NHS mail service for the Trust which includes adding, removal and suspension of NHSmail accounts. The NHSmail service includes a number of security features intended to prevent the transmission and storage of SPAM or malware through the platform. It also includes various security monitoring technologies to detect attacks or abuse of thesystem. *Microsoft ICO REGISTRATION* - Z6296785 Microsoft is a market leader in their trade – the incorrect use of data would have major implications for their reputation. 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.

	Teams has the following security features: - ISO27001 compliant - SSAE16 SOC - Integrated MDM Solution - Two factor authentication - Data is encrypted in transit and at rest

Step 6 - IG Review Panel

Date of IG Review Panel:		
Attendees:		
Project Ref and Description:		
Reviewer Name	**Issue**	**Mitigation**

Step 7: Identify and assess risks

Describe source of risk and nature of potential impact on individuals.
Include associated compliance and corporate risks as necessary.

Risk Rating

			Likelihood				
			Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
			1	**2**	**3**	**4**	**5**
Severity	**Catastrophic**	**5**	5	10	15	20	25
	Major	**4**	4	8	12	10	20
	Moderate	**3**	3	6	8	12	15
	Minor	**2**	2	4	6	8	10
	Negligible	**1**	1	2	3	4	5

Risk Ref	**Risk Description**	**Severity (S)**	**Likelihood (L)**	**Impact SxL**
	Patient could be admitted to the virtual group consultation in error	**2**	**3**	**6**
	Confidential information could be uploaded to the virtual group consult meeting in error	**4**	**2**	**8**

Step 8: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5					
Risk Ref	**Risk Description**	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
	Patient could be admitted to the virtual group consultation in error	All patients enter the meeting as a 'Guest' user which means all patients will enter a lobby and will be admitted by the host. Any patients that shouldn't be attending the consultation will be declined	Eliminated	No	Yes
	Confidential information could be uploaded by the host to the virtual group consult meeting in error	The host will be responsible for documentation shared at the meeting. Information cannot be downloaded by 'Guest' users.	Reduced	No	Yes

Step 9: Sign off and record outcomes

Item	**Name/date**	**Notes**
Measures approved by:	[redacted]	
Residual risks approved by:	[redacted]	
DPO advice provided:		
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	[redacted]	The DPO should also review ongoing compliance with DPIA