Oxford Health
NHS Foundation Trust

Data Protection Impact Assessment (DPIA)

Form (with Appendices)

Guidance information and definitions are available at the end of this document.

It is best practice to complete Part 1 and Part 2 of this DPIA whenever you are processing or changing the processing of personal data. **NB:** Pseudonymised data is viewed as personal data. Anonymised is not personal data and therefore does not require a DPIA. If no personal data will be collected or processed, you do not need to complete a DPIA.

If you answer yes to any of the questions in Part 1 - Screening Checklist, it is likely your DPIA is mandatory as you are partaking in data processing activity that could be high-risk and therefore you must complete Part 2 – Data Protection Impact Assessment.

Please submit your completed form to Information Governance.

ACTIVITY DETAILS

Title		
Oxevision patient monitoring system in Mental Health Impatient wards.		
DPIA Version Number	**2**	
Directorate	**Team/Area of Trust**	
Corporate	**SCAD**	
DPIA Lead Full Name	**DPIA Lead Contact Details**	
**********	**Email:**	**********
	Telephone:	**********
DPIA Author(s) Full Name (if applicable)	**DPIA Author(s) Job Title(s)**	
	Senior Project Manager	
Date DPIA Completed:	**27 June 2023**	
Proposed Start Date for Activity:	**In use**	

PART ONE – SCREENING CHECKLIST

Question	Answer Yes or No	
Are you processing (using) special category (sensitive) data? (Please see definitions in Appendix X)	Yes ☒	No ☐
Are you using new technology, or existing technology in an8 innovative way, whether technological or organisational?	Yes ☒	No ☐
Are you doing large scale profiling / processing?	Yes ☐	No ☒
Are you using biometric data for identification purposes?	Yes ☐	No ☒
Are you using automated decision making that may result in denying access to a service, making decisions that could deny someone access to a product, service, opportunity, or benefit or could be preventing them from exercising a right?	Yes ☐	No ☒
Are you processing (using) genetic data except when it is being used by an individual GP or health professional to provide healthcare directly?	Yes ☐	No ☒
Are you data matching? (i.e. where personal data is obtained from different sources, compared, and matched)	Yes ☐	No ☒
Are you doing invisible processing where the person does not know you are processing their data and you are unable to inform them?	Yes ☐	No ☒
Are you tracking someone's geolocation or behaviour?	Yes ☒	No ☐
Are you targeting children or other vulnerable people, profiling them, or offering online services directly to children?	Yes ☐	No ☒
Is there a risk of physical harm to someone's physical health or safety because of how you are processing personal information	Yes ☐	No ☒

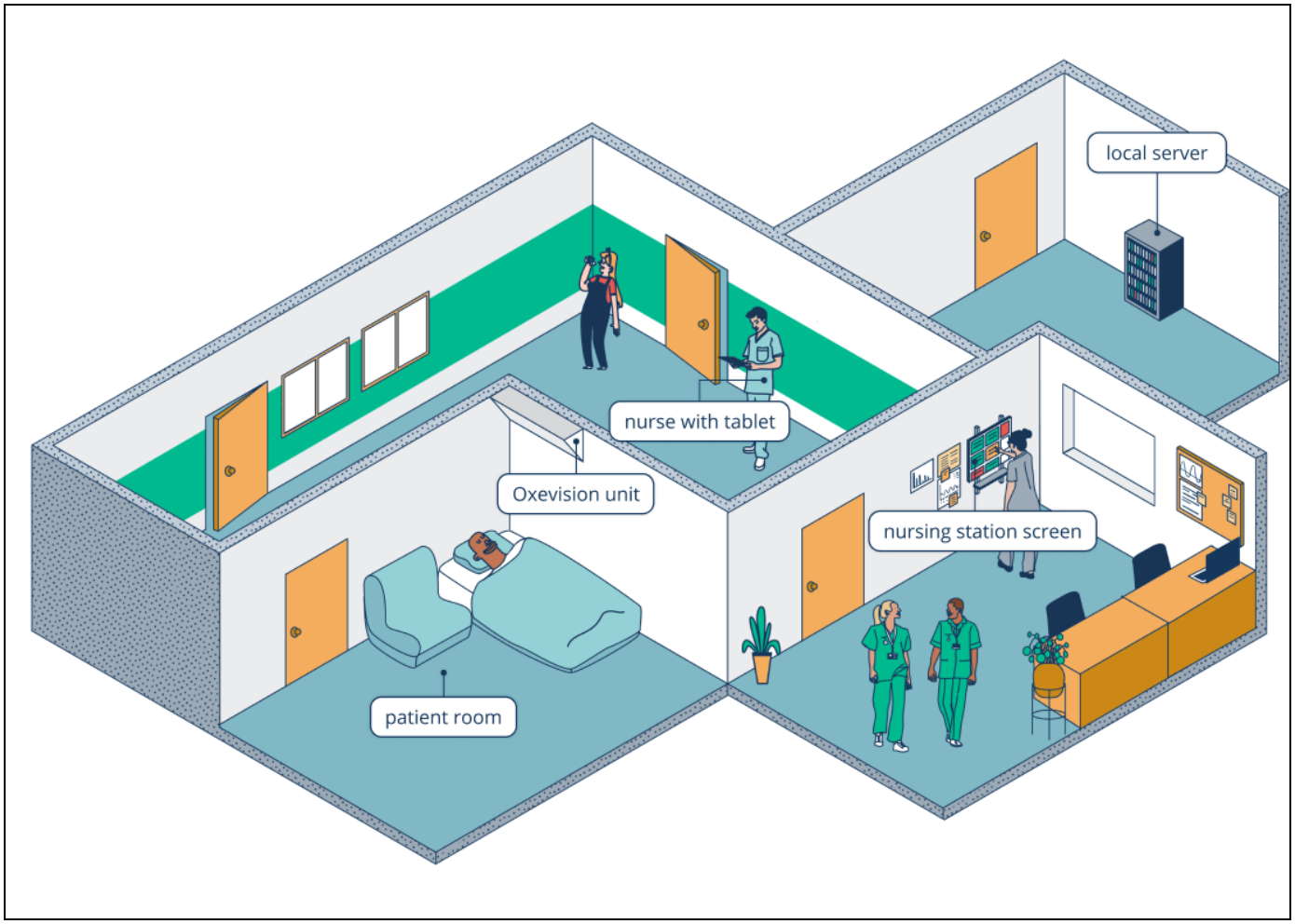
If you decide that a PART 2 DPIA is not required for your activity, please provide the justification for your decision.

PART TWO - DATA PROTECTION IMPACT ASSESSMENT (DPIA)

If you have answered yes to any of the questions in the Part 1 – Screening Checklist, your DPIA is likely to be mandatory and therefore you should complete this section and send it to Information Governance.

1. **ACTIVITY DESCRIPTION AND PURPOSE**

Briefly describe what you are doing / changing?
Installing Oxevision a contact-free vision-based patient monitoring systems into all Mental Health Impatient wards. Oxevision relays information to staff in realtime by using an infrared-sensitive camera housed in a secure unit installed in a patient's room. It enables clinicians to take a patient's pulse and breathing rate measurements completely contact-free and take a short, 15 second remote observation without disturbing their sleep. Through location and activity based alerts and warnings, Oxevision also notifies staff of activity that may indicate a patient needs help or assistance.
What is the purpose for the processing? i.e. The 'reason for' processing this personal information
To help to enhance patient safety on the ward. Oxevision is an assistive tool that enables staff to enhance and support patient safety in inpatient services by delivering non-contact measurement of physiological parameters such as pulse and breathing rate, some estimate of patient location, activity or behaviour data and some form of contextual video information either in real-time or through subsequent reviews. The use of Oxevision is intended to enhance existing clinical practice and not replace the need for nursing interventions.
What is the benefit of processing the personal information?
To increase patient safety and reduce patient harm on the ward and to improve ward staff working.
Please summarise how you are going to process the personal data.
Real time monitoring of patient bedrooms through the deployment of sensors and a camera. The Oxevision system captures both clear and anonymised images which are used by staff to support vital sign measurement and to respond to alerts respectively. Clear video data is retained for 24 hours before being overwritten, while anonymised data is held for the duration of the contract. Patients are asked to consent to the use of Oxevision in their bedroom at the point of admission onto the ward. Patient consent is recorded on the Trust Clinical Record System. Patients are made aware of the times (mostly overnight) that the camera maybe used to take patient observations for safeguarding purposes. Data is secured through a combination of measures restricting access to named persons only, encryption of the data, secure VPN and physical security of premises,



Oxevision unit: Housing unit containing the infrared-sensitive camera in a patient's room

Nursing station screen: Oxevision home screen showing room information such as alerts

Nurses tablet: Handheld tablet showing room information such as alerts and enabling clinical staff to take observations

Local server: Secure, local computer storage where Oxevision data is stored

Will you be using the data for any automated decision making? (i.e. making decision solely by automated means without any human involvement). If yes, please describe how the automated decision making will work.	**Yes ☐**	**No ☒**
Will you be monitoring data subjects e.g. using CCTV or other means of surveillance?	**Yes ☒**	**No ☐**
To enhance patient safety, reduce patient harm using technology to alert to multiple incidents (bedroom occupation, bathroom access, and edge of bed, etc). To improve patient and staff experience through remote physical health monitoring.		

DATA REQUIREMENTS

Whose personal data will be processed?			
Staff (including employees, flexible workers, agency workers, honorary contracts, students)	☒	Patients/service users	☒
Members of the public	☐	Other (Please describe):	☐
How many individuals' data will be processed?			
1-100	☐	1,001-5,000	☐
101-500	☒	5,001-10,000	☐
501-1,000	☐	10,001+	☐

What type of personal data are you using? Please see the data type descriptions in Appendix A and list examples of the data e.g. patient names, date of birth, gender **NB:** Pseudonymised data is viewed as personal data. Anonymised is not personal data and therefore does not require a DPIA.
Personal Data List: The Oxevision system captures both clear and anonymised images
Sensitive Data List: The Oxevision system captures both clear and anonymised images Health data relating to vital signs and observation of health status
Criminal Offence Data List: None
Where/Who are you getting the data from? Please use descriptive labels such as Participants, Job Titles, Team, organisation names, system names rather than the names of individuals
The patient occupying the bedroom.
How will you get the data? E.g. secure file transfer, directly from a database, collected from a study participant etc.
Real time data feed providing alerts and the ability to view into a patient's bedroom from a monitor screen and/or tablet. Clear video data is retained for 24 hours before being overwritten, while anonymised data is held for the duration of the contract.

Data is secured through a combination of measures restricting access to named persons only, encryption of the data, secure VPN and physical security of premises,

2. DATA STORAGE, RETENTION AND SECURITY

Who will have access to the data? Please use descriptive labels such as Job Titles, Team names rather than the names of individuals
The staff on the ward and certain authorised staff working for the system provider Oxehealth.
How will the data be protected?
Whilst the data is being recorded it will be stored on the local computer equipment securely at Impatient Ward sites (local secure server and network attached storage). In these storage locations, all personal data will be encrypted at rest to the AES256 standard. All data stored on the secure cloud servers will be encrypted at rest to the AES256 standard. All data transmission between local computer equipment at Inpatient ward sites will take place over a secure virtual private network (VPN), which ensures communication between authenticated devices only, using secure socket layer (SSL) encryption to the AES256 standard. Any data transfer over the internet will use SSL encryption to the AES256 standard. During transfer of the Personally Identifiable Salient Video Data back to Oxehealth's secure facility on network attached storage devices, the servers will be always accompanied by a member of the Oxehealth team or a trusted courier.
Where are you going to store the data?
On servers located on each ward site, Oxehealth's secure remote hosting facility, provided by Amazon Web Services (located physically in the UK) and at Oxehealth's secure servers at Oxehealth's premises.
What measures will be in place to ensure the data is accurate?
The data is a real time feed and when stored is time and date stamped.
How long will you keep the data and why?

Until the end of the contract with Oxehealth, when no longer required or when requested to be deleted, whichever is earlier.		
Do you need to share the data with a 3rd Party?	**Yes ☒**	**No ☐**
Data is shared with the system provider (Oxehealth).		
Please also give details of how will you share the data? All data transmission between local computer equipment at Inpatient ward sites and Oxehealth will take place over a secure virtual private network (VPN).		
Does Oxford Health have an Information Sharing Agreement in place with the 3rd Party? (If yes please attach a copy).	**Yes ☐**	**No ☒**
Is any of the data going to be sent or stored outside of the UK/EEA?	**Yes ☐**	**No ☒**
If yes, where is it going/being stored?		
How are you informing the individuals whose data you are processing about their rights? E.g. Patient Information Leaflet, Trust Privacy Notice.		
All patients admitted to an inpatient mental health ward are informed about the Oxevision system and asked by ward staff to consent to the use of Oxevision in their bedroom. Patients are handed a patient leaflet about Oxevision which explains their rights and how their privacy is safeguarded.		
What measures will be in place to eliminate or reduce risks of data breaches?		
The Trust already have strict practices surrounding data confidentiality and privacy of patients, governed by the NHS Code of Confidentiality and the Caldicott Principles. No additional personal data will be made available to Trust staff because of this project.		

The local secure server will be located at each Ward site and will should be provided with appropriate physical and electronic access restricted to authorised Trust or Oxehealth personnel by the Trust Estates and Facilities team. Trust staff are bound contractually by the Caldicott Principles and the NHS Code of Confidentiality. In addition, the video data held on a local secure server is in a proprietary format which could not be viewed with publicly available software. The risk of data being disclosed or lost by a member of Trust staff is therefore deemed to be very low.

To avoid a potential data leak due to theft or malicious electronic attack (and therefore mitigate the risk of accidental damage to or loss of data), Oxehealth have several preventative measures in place, including:

- A detailed code of conduct for Oxehealth staff surrounding the use and security of patient data – this clearly states that data should not be used for publicity, information about patients should not be discussed outside of the office and no data should be copied off company servers
- The local secure server, and the data contained therein, is held within a secure area at [Partner]Oxford Health NHS Foundation Trust Mental Health sites.
- Portable storage devices are always accompanied in transit by Oxehealth staff or a secure courier
- All personal data is encrypted prior to being stored and remains encrypted to industry standard AES256 until placed on Oxehealth servers in the secure Oxehealth storage facilities
- All electronic communication of personal and non-personal data uses industry standard encrypted and authenticated protocols
- Personally Identifiable Salient Video Data storage is in a secure room with limited keyholder access in a building with 24-hour security guards. This is backed up at Oxehealth, until secure deletion.
- Oxehealth's secure cloud servers provided by Amazon Web Services adds a second layer of encryption to Staff Identification Data
- Oxehealth's network is protected with a perimeter UTM firewall, scanning and protecting the gateway from external threats (including intrusion prevention, anti-virus, anti-spyware and botnets)
- Network storage and fileservers are only accessible from the Oxehealth IP range, using individual logons only
- All data collected and generated by the Oxehealth system is anonymised as far as possible and personally identifiable data collection is kept to a minimum only where necessary to provide the service to the contracted standard.

Have you consulted with the people who will be impacted by the processing activity?	**Yes ☒**	**No ☐**

All patients are asked to consent to the use of Oxevision in their bedroom on admittance to the ward. Where a patient objects the Oxevision system is turned off in their bedroom and they are monitored in person instead.

LAWFUL BASES FOR PROCESSING

What is your lawful basis for processing? Please see the lawful basis for processing descriptions in Appendix B.	
Article 6 – Personal Information Please click the box next to the lawful basis you are using	
Article 6(1)(a) Consent	☒
Article 6(1)(b) Contract	☐
Article 6(1)(c) Legal Obligation	☐
Article 6(1)(d) Vital Interests	☐
Article 6(1)(e) Public Task	☐
Article 6(1)(f) Legitimate Interests	☐
Article 9 – Special Category (Sensitive) Information Please click the box next to the lawful basis you are using	
Article 9(2)(a) Explicit Consent	☒
Article 9(2)(b) Employment, Social Security & Social Protection	☐
Article 9(2)(c) Vital Interests	☐
Article 9(2)(d) Not-for-Profit Bodies	☐
Article 9(2)(e) Made Public by the Data Subject	☐
Article 9(2)(f) Legal Claims or Judicial Acts	☐
Article 9(2)(g) Reasons of Substantial Public Interest	☐
Article 9(2)(h) Health or Social Care	☐
Article 9(2)(i) Public Health	☐
Article 9(2)(j) Archiving, Research and Statistics	☐

3. CONTRACT INFORMATION

Does what you are doing / changing involve a contract? If yes, please tick which type of contract and attach as copy of the contract to your submission to Information Governance?		**Yes ☒**	**No ☐**
NHS Framework Contract	☐	Employment Contract	☐
Off NHS Framework	☐	Other	☒
Service Provision	☐		

RISK ASSESSMENT

The level of risk is scored out of 25. A score of 0-5 is attributed to both the impact on the rights and freedoms of the individual, and the likelihood of those rights and freedoms being compromised. The two scores are then **multiplied**

to create the composite risk score using the risk matrix below. This should be recalculated in the final columns to consider proposed solutions/actions. Appendix 3 contains some examples of common information risks.

Risk	Description	Risk score see matrix below			Proposed solutions/actions	Revised Risk score see matrix below		
		Impact	Likelihood	Risk Rating		Impact	Likelihood	Risk Rating
1	Cyber Attack	3	1	3	Patient monitored in person instead	1	1	1
2	Identification of a patient by an Oxehealth member of staff	3	1	3	The risk of identification cannot be ruled out but is very low. In the event of a member of the Oxehealth team being able to identify a patient the Trust will be consulted and the default action is to delete all data relating to that patient.	1	1	1
3	System Failure	1	3	3	Patient monitored in person instead	1	1	1
4	Data is retained longer than necessary	2	1	2	All data files are date and time stamped so that retention can be tracked, and reviews of data stored are undertaken regularly. At least twice per year, Oxehealth provides the Trust with a Salient Video Data Report which confirms the purpose, principles and review process for any Personally Identifiable Salient Video Data collected for the Trust and a log of the personal data retained, reasons for retentions and date of next review.	1	1	1

Risk	Description	Risk score see matrix below			Proposed solutions/actions	Revised Risk score see matrix below		
		Impact	Likelihood	Risk Rating		Impact	Likelihood	Risk Rating
5	Personal data other than the patients face is accidentally shared with Oxehealth	3	2	6	There are on-screen warnings to staff to avoid personal data on all Oxehealth software functions where data may be accidentally shared. Staff are also trained on the use of the software as part of the service. Further a redaction process within the customer support process ensures that any personal data accidentally shared is removed from all Oxehealth records, and not further processed by Oxehealth .	1	1	1

Risk matrix

	Impact (How bad it may be)		Likelihood (The chance it may occur)			Risk Rating				
						1	2	3	4	5
5	Catastrophic	**5**	Almost certain	CONSEQUENCE	5	**5**	**10**	**15**	**20**	**25**
4	Major	**4**	Likely		4	**4**	**8**	**12**	**16**	**20**
3	Moderate	**3**	Possible		3	**3**	**6**	**9**	**12**	**15**
2	Minor	**2**	Unlikely		2	**2**	**4**	**6**	**8**	**10**
1	Negligible	**1**	Rare		1	**1**	**2**	**3**	**4**	**5**

Likelihood (L) x Impact (I) = TOTAL RISK RATING

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