Data Processing Impact Assessment (DPIA)

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

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.

Submitting controller details

Name of controller	Leicestershire Partnership NHS Trust
Subject/title of DPO	Oxevision
Name of controller contact /DPO (delete as appropriate)	Sarah Ratcliffe Head of Data Privacy/Group Data Protection Officer (NHFT/LPT) [I/S]
DPIA	DPIA0047

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Leicestershire Partnership NHS Trust wishes to deploy the Oxehealth Software & Oxehealth Services to improve and supplement its patient care and safety monitoring regimes. An 8-week pilot has been proposed within the Trust to trial the use of Oxevision monitoring equipment on Ashby Ward which is a female Mental Health Inpatient Ward at the Bradgate Unit. The pilot aims to enhance and improve patient experience at night by reducing the disturbance caused by intermittent observations. There are additional anticipated benefits which include: • Reduce self-harm, including ligatures. • Reduce Assaults - Reduce incidences and early warning signs. • Reduce restrictive interventions. • Improve physical health monitoring – early detection of deterioration. • Improve staff experience. It has been fed back by consultants and by patients that disturbance at night of taking observations does impact on patient recovery whilst in hospital. The type pf processing proposed in this project, is that digital video cameras will be used to record to enable physical observations to be taken from 11pm until 0730 am by completing intermittent level 1(hourly) and level 2 (10/15min) observations. This will enable patients observations to be taken without disturbing patients. A Data Protection Impact Assessment was identified as required due to the introduction of a new technology which generates and processes the health data of vulnerable patients. Whilst CCTV is used throughout Leicestershire Partnership NHS Trust facilities and in seclusion rooms, it is not currently used in the patient bedrooms or ensuites as proposed to be used for the Pilot project.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

There are three main types of data that will be processed during the Pilot detail on storage, handling and deletion for each data type is included against each type below. All video data is anonymised and not linked to an individual, the feed of Clear Video Data is only accessible in 15 second intervals to enable observations to take place. Where clear video data is requested and viewed repeatedly by a member of staff an alert is generated to enable confirmation that access was warranyted.

Clear Video Data

Raw video footage of patients, staff and visitors generated by the cameras as part of the Oxevision platform.

Usage and Purpose

- Automated processing of the camera feed by the Oxevision platform to generate movement alerts data and vital signs measurement data.
- Viewed by clinical staff for up to 15 seconds while taking breathing & pulse rates to confirm they are accurately taken from the correct individual.

Storage & Retention

- Clear Video Data will be stored on an Oxehealth managed secure server physically located at an LPT site for up to 24hrs after which it is automatically deleted by the software.
- In the event of information being requested from Oxevision by LPT, clips would be taken and retained for a total of 30 days within the solution.
- Any clips being required to be held longer than 30 days would be transferred via the Egress secure email solution All data will be stored on Egress UK servers and will be encrypted in transit and at rest. Data deletion from Egress is automatic after 28 days. Egress will be used if any CVD is required to be transferred to them for serious incident review – I believe this is included in the SOP, so Egress will be a sub-processor. All data will be stored on Egress UK servers and will be encrypted in transit and at rest. Data deletion from Egress is automatic after 28 days.

Anonymised Blurred Video Data:

Data which is anonymised (blurred) Video Data is created by irreversibly blurring the visual data feed from the camera. Individuals cannot be identified from this data alone and stored data is further pseudonymised.

Usage and Purpose

- Viewed by clinical staff for 15 seconds when viewing an alert, or up to 10 minutes when using functionality to replay the last alert (displays 5 minutes before and 5 minutes after the alert).
- Clinical staff can additionally view up to 30 minutes of blurred video from the previous 4 days for a specific room and timeframe to investigate a serious incident as part of retrospective review.
- Encrypted and pseudonymized data processed by the Oxehealth team to:
  - Support initial configuration of the software (blind running)
  - Provide standard maintenance (monitor performance and address issues)
  - Improve the performance of the product in use by the customer and ensure there is no negative impact from any changes made.

Storage & Retention

- Stored on the local secure server at customer site for 24 hours and automatically deleted by the software.
- Encrypted and pseudonymized data stored in AWS secure cloud servers and automatically deleted by the implementation of AWS retention policies.

Staff Identifiable Data

As part of user identification and to access some Oxehealth software modules for digital observations and retrospective review, the names of individual members of staff are processed and stored within the local secure server. Staff Identification data which is limited to name and email address is also recorded as part of system configuration for reporting purposes.

Usage and Purpose

- Processed by 3rd party software (Amazon SES or Egress) to email reports (e.g. activity tracker, vital signs trends, sleep insights) to clinical staff.
- Manually entered by clinical staff to access some software module functions and to access and share reports.
- Processed by the system to record report activity to the GUI logs to monitor access by clinical staff to some Oxehealth software modules and to provide an audit trail of clinical staff adding, viewing and modifying reports

Storage & Retention

Staff name and email address will be stored in the following ways:

- Stored on the local secure server and retained while there is an associated record and for a further 24 hours after the associated record is deleted.
- Stored in Amazon Web Servers (AWS) secure cloud servers for an additional 7 days after the data is deleted from the local secure server and automatically deleted by AWS retention policies.
- Where reports are emailed via Egress they are stored in AWS only while the transaction takes place.
- Reports are stored in Egress for 30 days and then automatically deleted.
- Manager data is stored within Gitlab (on a USA server) until the end of the customer contract and deleted.

Data sharing:
Each data type includes details of how they will be stored, retained and shared within. A list of sub processors used by Oxehealth are included below:

- Amazon Web Servers UK Based
- Gitlab USA based
- Egress UK based

Type of data processing that need further consideration:
High risk processing has been identified through the 24/7 video monitoring of patients using Clear Video Data within their bedrooms and bathrooms. This data will include clear video data where a patient will be viewable in short intervals to support the taking of remote observations.

The use of Gitlab to store staff identifiable data which will store data in the USA needs to be considered.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
The data is a mixture of special category patient data captured via video and observations and personally identifiable data for staff data. Ongoing monitoring of data subjects will take place every day during this pilot between 11pm until 0730 am and special category data of data subjects will be captured as clear video data and patient observation data. Clear video data will be deleted after 24 hours by LPT and Oxevision, unless it has been approved that they are required to be retained for a patient safety incident investigation. In the event of information being requested from Oxevision by LPT, clips would be taken and retained for a total of 30 days within the solution. This data processing will be carried out on the Ashby Ward during the 8-week period of the pilot.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they 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? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Individuals whose data would be processed using this technology will be patients in the care of LPT who reside within the Ashby Ward. Ashby Ward is a 21 bedded female inpatient ward providing care for adults with acute mental health problems. Patients have the ability to withdraw their consent for recording as the intention is to support patients to have observations taken without disturbing them at nighttime. The capture of data in this way is a new approach for the Trust and due to it being a new technology will be new to patients. There is a privacy notice available to all patients on the LPT website and the intention is for this to be updated to provide details of the technology. Patient materials will be updated to support patient users to understand the benefits of the technology and to support them to make an informed decision. The technology is an emerging innovation in the field of patient observations and its use in the proposed pilot would require the use of a new technology within the Trust. The technology has been reviewed by the Trust Cyber Team who have not identified any security concerns but have identified that Muti Factor Authentication is not available. The system will need to be added to the Policy exception list for MFA and escalated to the SIRO. Below are summary details of the security and medical certifications of the technology: • The Oxehealth Vital Signs software is a class IIa medical device in the UK and EU. Vital Signs Basic UDI-DI for identification in Eudamed: 506075145VITALSIGNSFF • The Oxehealth software and provided hardware infrastructure are subject to twice annual penetration testing using CREST accredited external auditors. • Vulnerability tooling scans all libraries and packages within the software against the NIST and other vulnerability databases during development and Nessus grey box scans of the system are carried out and actioned as part of release testing within a regular release cycle. • Oxehealth regularly scans for vulnerabilities and holds Cyber Essentials Plus certification for its internal infrastructure. There are nationally reported concerns within news media over the potential for privacy intrusion when using this type of technology to monitor vulnerable patients

and these concerns have been taken into account as part of the DPIA review of the Pilot project.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Leicestershire Partnership NHS Trust wishes to deploy the Oxehealth Software & Oxehealth Services to improve and supplement its patient care and safety monitoring regimes.

An 8-week pilot has been proposed within the Trust to trial the use of Oxevision monitoring equipment on Ashby Ward which is a female Mental Health Inpatient Ward at the Bradgate Unit.

The intended effect on individuals is to enhance and improve patient experience at night by reducing the disturbance caused by nursing staff undertaking intermittent observations at nighttime. Observations at nighttime when patients are sleeping, washing or in the bathroom are currently undertaken by staff shining torch through the door to locate the patient and often to enter the room to take physical observations. The proposed technology gives opportunity to be completed without staff entering the room. Reducing disruption.

There are additional anticipated benefits which include:

- Reduce self-harm, including ligatures.
- Reduce Assaults - Reduce incidences and early warning signs.
- Reduce restrictive interventions.

- Improve physical health monitoring – early detection of deterioration.
- Improve staff experience.

It has been fed back by consultants and by patients that disturbance at night of taking observations does impact on patient recovery whilst in hospital.

The type pf processing proposed in this project, is that digital video cameras will be used to record to enable physical observations to be taken from 11pm until 0730 am by completing intermittent level 1(hourly) and level 2 (10/15min) observations. This will enable patients observations to be taken without disturbing patients.

Step 3: 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?

Consultation has been completed prior to the decision taken to undertake a pilot, detail of the different types of consultation is detailed below:

- The Trust Executive Management Board which includes senior clinical representation has been consulted and asked to support the Pilot subject to the approval of the DPIA and the identified mitigating actions. Approval was received on the 2nd of August.
- The pliot is being shared for consultation through lived experience patient steering groups and patients on the pilot ward have already been contacted to provide feedback.
- The pilot has been reviewed by senior operational and clinical leads in the Mental Health Directorate and it has been agreed that the pilot would be beneficial to support any decisions on the future use of this type of technology
- A number of NHS Organisations currently use the technology and the details are included on their website: https://www.oxehealth.com/ The Trust has been in contact with Essex Partnership Trust to gain an understanding of how they have approached the use of the technology.
- During the DPIA process senior clinicians within the Trust have been contacted to discuss the approach to managing consent for data subjects and the processes for patients in seclusion.
- Cyber Security and Data Privacy expertise has been sought from internal stakeholders to review the technology prior to the completion of the DPIA.

- Demonstration of the product and the specific proposed configuration was presented to the DPO.
- Information has been provided to support the Pilot project and the completion of this Data Protection Impact Assessment by Oxehealth the developers of Oxevision who would act as data processor if the project gains full approval. The data processor has confirmed that they have undertaken the following types of consultation on their product:
    - *In addition to internal stakeholders in engineering, product and compliance, Oxehealth engages with experts by experience, NHS customers, the Nursing directors Forum and the CQC on the use of the Oxevision platform, and any feedback on the data generated by the system and how it is used is included in ongoing risk assessment and helps to inform the controls which are implemented. Oxehealth additionally seeks advise from supervisory authorities and legal counsel for best practice.*

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Patients on the Ashby Ward including those in seclusion will be asked for their consent to be included in the pilot. There is a privacy notice available to all patients on the LPT website and the intention is for this to be updated to provide details of the technology. Patient materials will be updated to support patient users to understand the benefits of the technology and to support them to make an informed decision on their consent to this as part of their treatment pathway.

Patients have the ability to withdraw their consent for recording as part of their treatment as the intention is to support patients to have observations taken without disturbing them at nighttime.

For patients who consent to treatment in this way the legal basis for capturing Special Category Personal Data provided to the Trust for the purpose of healthcare delivery, management and treatment Article 9(2)(h)

"necessary for the reasons of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional."

For patients in seclusion who do not have capacity the legal basis is Article 9(2)(c) which permits you to process special category data if:

"processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent".

The intended effect on individuals is to enhance and improve patient experience at night by reducing the disturbance caused by nursing staff undertaking intermittent observations at nighttime. Observations at nighttime when patients are sleeping, washing or in the bathroom are currently undertaken by staff shining torch through the door to locate the patient and often to enter the room to take physical observations. The proposed technology gives opportunity to be completed without staff entering the room. Reducing disruption.

The functionality will be limited to where the devices are installed.

The system access is limited to the nurse in charge, ward sister, deputies or CDM. The data itself will be minimised to viewable 15 second clips of clear video data to minimise the amount of identifiable data captured.

The staff member will show the patient the devices and provide the patient with a leaflet along with their welcome pack.

Consent will be reviewed daily and those patients wishing to withdraw their consent will have their rights respected unless they are in seclusion without capacity, and it is in their or others vital interests to undertake videoed observations. This is in accordance with the Mental Health Act Code of Practice:

https://assets.publishing.service.gov.uk/media/5a80a774e5274a2e87dbb0f0/MHA_Code_of_Practice.PDF

"Staff should balance the potentially distressing effect on the individual of increased levels of observation, particularly if these are proposed for many hours or days, against the identified risk of self-injury or behavioural disturbance. Levels of observation and risk should be regularly reviewed, and a record made of decisions agreed in relation to increasing or decreasing the observation."

Consent to record when a patient is in seclusion will be handled under section 9.5 of the LPT Seclusion Policy:

https://www.leicspart.nhs.uk/wp-content/uploads/2023/10/Seclusion-and-long-term-segregation-Policy-V16-Exp-April-2027.pdf

"The decision to seclude must be explained to the patient in an appropriate manner at the first available opportunity, outlining the particular behaviour which has necessitated the use of seclusion. This explanation must be given in a manner appropriate to the individual's needs; this may include the provision of an interpreter, hearing assistance or other means of communication aids. The discussion must be detailed in the patient record and include supporting information regarding the patients understanding."

A data processing agreement will be in place with Oxevision. This agreement will include provision for audits and confirmation of annual security checks.

International data transfers will be safeguarded through data processing agreement and through data minimization.

Step 5: Identify and assess risks including measures to reduce risk

Oxevision Risk Assessment Final.xlsx

Step 6: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	[I/S], Director of Finance/SIRO	Actions identified in ISRA document to be monitored via Data Privacy Group
Residual risks approved by:	SIRO and Caldicott Guardian	
DPO advice provided:	Risk actions identified within the risk log must be completed.	Processing of data for the pilot can proceed.

Summary of DPO advice: The DPO has requested a change to the processes around the capturing of consent for patients in seclusion. This change has been accepted by the Clinical Service and reflected within the SOP.		
DPO advice accepted or overruled by:	Advice accepted by Andres Patino	
Comments: SOP Updated with change.		
This DPIA will kept under review by:	Head of Data Privacy/Group Data Protection Officer	Results will be fed into the Data Privacy Group
SIRO Approval Signature:		Date:
Caldicott Approval Signature:		Date: