

Data Protection Impact Assessment (DPIA)

Why do I need to complete a DPIA?

This process is a mandated legal requirement of data protection legislation to ensure that privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.

When do I need to complete a DPIA?

This document must be completed for any proposed, new or change in process, service, technology or project which pertains to utilise personal identifiable information. It must be completed before change, implementation or procurement.

Who should complete a DPIA?

The DPIA should be initiated and completed by either the relevant Project Manager, System Manager, General Manager or Information Asset Owner in the area proposing the change.

It is advisable to include the following in the completion of this form:

- Trust Data Protection Officer (DPO) and Information Governance Team
- Relevant stakeholders
- IT & Information Security Team
- Any data processors (including 3rd party suppliers)
- Legal advisors or other subject matter experts, where relevant

Following completion of the DPIA, it may also be necessary to consult with the ICO where measures cannot be taken to reduce any residual high risk of implementation.

The DPIA must be approved and signed by the organisations Data Protection Officer (DPO) prior to project or system go live

What Next?

Please complete the screening questionnaire on the next page, if you answer yes to any of the screening questions you will be required to complete the full DPIA with as much detail as possible and return the completed form to tevv.dpia@nhs.net

Further guidance on DPIA can also be found on the Information Commissioner's website www.ico.gov.uk

Section A - Data Protection Impact Assessment Screening Questionnaire

To confirm whether a full DPIA is required for your new / or change in service which involves the use of personal identifiable information please answer all the questions below.

Project Name	Oxevision - Vision Based Patient Monitoring System provided by Oxehealth
DPIA number:	CSI065
Project Description	Oxehealth is a Digital Care Assistant (DCA) system (non-contact technology) it supports clinicians in maintaining patient safety via the use of infra-red sensors and HD camera technologies in a fixed installation unit. These are linked to an interface at the nurse station in the form of a computer screen and portable tablets. It is implemented within ward patient bedrooms and seclusion rooms. Oxehealth DCA technology provides: i) Activity alerts – Real-time alerts based on continuous safety monitoring. ii) Vital Signs measurements – Spot measurements of pulse and breathing rate. iii) Activity Reports – Timeline summary of patient activity detected in a room, including time in bed, room (but not in bed), out of room.
Name and Job title:	[I/S] – Nurse Consultant
Date:	29/11/2023

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.

VBPMs are assistive tools that enhance and support patient safety in inpatient services. The purpose of VBPMs is to support patient and staff safety in inpatient services.

Oxevision is a contact free, VBPMs for use in single occupancy rooms on inpatient wards. It is an assistive tool to enhance and support patient safety and clinical practice and does not replace the need for nursing interventions. It provides clinical teams actionable data to support planning patient care and intervening proactively to help their patients. It includes a regulated medical device that incorporates an infrared sensitive camera.

It helps staff to visually confirm a patient is safe and measure their pulse and breathing rate without disturbing their sleep. It provides staff with notifications to predefined activities within a room (e.g., a patient getting out of bed) and information on a patient's active and resting periods (e.g., how long a patient spent in bed, how frequently they went to the bathroom overnight). Staff on the ward receive information and notifications on a screen in the nursing office or tablet devices they can carry on the ward. Staff on the ward can see a clear image of the room for up to 15 seconds only when checking a patient's pulse and breathing rate. They can see an anonymised, blurred image of the room for up to 15 seconds only when a notification has been received to

support the completion of an additional safety check. Usage reports for Oxevision can be provided to support governance and auditing processes within organisations.

VBPMS cannot and should not replace positive and therapeutic engagement with patients and the visible presence of staff within inpatient settings. Staff must remain responsible for the patient and clinical judgement must be used at all times. Emergency intervention where self-harm is suspected should not be delayed by first checking the VBPMS.

As mentioned, the primary purpose of VBPMS is to assist staff in enhancing and supporting patient safety in real-time. The data requirements of the system requires that Clear Video Data is recorded to be able to clearly identify the occupant of the room being reviewed when taking physical observations to enable correct identification of the person being assessed. Whilst not their primary purpose, VBPMS can assist in providing data (including but not limited to video data) to support incident investigations. In doing so, these systems have the ability to support patients, carers, staff and organisations to learn from these events – therefore providing assurance that the right actions are taken to prevent them from occurring in the future.

Specifically, use of these data is limited to supporting serious incident investigations where a patient has come to serious or catastrophic harm as a result of a patient safety incident. These data can support Patient Safety Incident Investigations (PSIIs) and Patient Safety Reviews (PSRs) as part of the Patient Safety Incident Response Framework (PSIRF).

Data access, recording, usage, disclosure, retention, and deletion is to be clearly recorded within this Data Protection Impact Assessment (DPIA), Privacy Notice, patient information materials and other relevant documents to ensure accurate and consistent messaging around use of personal data.

Considerations must be given around human rights and ethical issues and the use of VBPMS to support saving lives and establishing this as a standard way of delivering a safe service.

Serious and untoward incidents occur within inpatient settings; bedrooms are a particular area of concern. Despite significant developments in how services identify and dynamically manage risk, it remains the case that any process of risk assessment/management no matter how robust or expertly delivered will at times be unable to predict all eventualities.

There are numerous examples from across the country where catastrophic events have been avoided among such individuals when staff use a VBPMS as an assistive tool.

There is a challenge in the management of consent, specifically regarding the Mental Capacity Act and the Mental health Act, especially when the patient is in an acute phase of illness, most specifically at the point of admission to hospital.

In respect of privacy, a balance is required based upon the VBPMS versus the current practice of regular hourly (or more frequent) sleep checks or staff undertaking specialist observations of patients in their bedrooms during which they leave the bedroom door open continuously to see if the patient is safe.

Providing safe inpatient environments crucially relies upon constantly being aware of a range of potential risks, including risks posed by others receiving healthcare within the same setting (i.e., sexual safety, exploitation, bullying/harassment, the principles of trauma informed care etc.).

Vision-based patient monitoring systems (VBPMs) cannot and will not replace positive engagement with patients and the visible presence of staff within inpatient settings. Information that is captured by the VBPMs, and provided to clinicians, is of a nature that helps clinicians in the management of health and safety of patients within the ward environment – for example, by providing staff with vital information and insights to facilitate earlier intervention to reduce the probability of an incident of harm occurring.

Open letter from the NHS about the use of VBPMs and the undertaking of the group for now and in the future.



Use of Vision Based
Monitoring Systems ii

The Trust currently adopts the single approach of consent, and the position of this consent versus explicit consent will be reviewed regularly and discussed and agreed in conjunction with the stakeholders and most especially carers and service user groups. The use of Oxevision will be carefully considered on a case by case, patient by patient basis to ensure that any decision to use such systems has a legitimate aim and is both lawful and fair. Their use must also be proportionate to the aim.

The adopted consent model requires that:

For the purposes of safeguarding and maintaining patient safety and pending a comprehensive risk assessment, all service users are opted in upon admission for the first 72 hours; patients must be informed of how to decline (opt out) the use of Oxevision in their care should they wish to do so.

Service users and carers must be informed and told of the use of VBPMs including the use of video data, both on admission and throughout their stay in hospital.

Service users can raise questions and concerns, and there should be regular opportunities for service users to be engaged by staff in conversation about their questions and concerns.

The service user can request to opt out at any time.

Any request to opt out by a service user should be discussed with the multi-disciplinary team, the services user, and carers (where practicable).

Where it is assessed that the service user lacks capacity regarding consent, all decisions should take place within the guidance of the best interest process (MCA 2005). This would facilitate personalised consideration of individual preference, safety/risk, and other alternatives. This **MUST** be documented within the patient's notes within the patient care record system, alongside an updated safety summary.

Patient advocacy should also be taken into consideration for any decisions, which must be clearly documented within the clinical records.

Within 72 hours on the ward the MDT will reach a clinical decision regarding the use of the VBPMs for the patient based upon a balanced view of the following factors:

Data Privacy Impact Assessment

- Reassessment of the mental capacity status of the patient in relation to their understanding of the use and implications for them of the VBPMs.
- The current risk of patient harm to self and others.
- Any particular risk of re-traumatisation based on patient history, or other potential harms to the patient from the use of VBPMs.
- The availability and use of alternative care interventions and other least restrictive approaches.
- MDT meeting should also consider whether the patient is admitted informally or formally (subject to the Mental Health Act).

Questions	Yes	No
Will you collect new information about individuals or compel them to provide information about themselves?	X	
Will information be shared to organisations or people who have not previously had access to the information? (including processing by 3 rd parties)	X	
Will you use information about people for a purpose that it is not currently used for, or in a way it is not currently used?	X	
Will you use systematic and extensive profiling or automated decision making to make significant decisions about people?		X
Will you process special category data (sensitive data) or criminal offence data on a large scale? (<i>Sensitive includes health information</i>)	X	
Will you systematically monitor a publicly accessible place on a large Scale?		X
Will you be using any new technologies or technologies which might be perceived to be privacy intrusive e.g. processing biometric or genetic data?	X	
Will you use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?		X
Will you carry out profiling on a large scale?		X
Will you combine, compare or match data from multiple sources?		X
Will you process personal data without providing a privacy notice directly to the individual?		X
Will you process personal data in a way which involves tracking individuals' online or offline location or behaviour?	X	
Will you process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?		X
Will you process personal data which could result in a risk of physical harm in the event of a security breach?	X	

Data Privacy Impact Assessment

If you have answered **YES** to any of the questions above, **you must complete the full DPIA on the next page** and return to the Information Governance Team at tewv.dpia@nhs.net

If you have answered **NO** to **ALL** questions, **you are not required to complete a full DPIA**. However, Information Governance must record all decision making regarding DPIA, please return your completed screening questionnaire to the Information Governance Team at tewv.dpia@nhs.net

Section B - Full Data Protection Impact Assessment (DPIA)

Form completed by:

Name:	[I/S]
Job Title:	Nurse Consultant
Signature:	[I/S]
Date:	15/03/24 updated 15.7.24

Name of System / Project:	Oxevision - Vision Based Patient Monitoring System provided by Oxehealth
Data Controller details:	TEWV
Data Processor details:	Oxehealth
Objective:	To enhance and support patient safety

Background: Why is the new system / change in system required?	A Vision Based Patient Monitoring System (VBPMS) is an assistive tool that enhances and supports patient safety within inpatient services. VBPMS are assistive tools that enable 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 (which may be blurred) either in real time or through subsequent reviews. The use of these systems is intended to enhance existing clinical practice and not replace in any way the need for nursing interventions. The Trust currently only uses one VBPMS, supplied by Oxehealth and referred to as Oxevision, part of which is also classified as a Class IIa medical device and therefore is regulated by the Medicines and Healthcare products Regulatory Agency. Oxevision is a contact free, VBPMS for use in single occupancy rooms on inpatient wards. It is an assistive tool to enhance and support patient safety and clinical practice and does not replace the need for nursing interventions. It provides clinical teams actionable data to support planning patient care and intervening proactively to help their patients. It includes a regulated medical device that incorporates an infrared sensitive camera. It helps staff to visually confirm a patient is safe and measure their pulse and breathing rate without disturbing their sleep. It provides staff with notifications to predefined activities within a room (e.g., a patient getting out of bed) and information on a patient's active and resting periods (e.g., how long a patient spent in bed, how frequently they went to the bathroom overnight). Staff on the ward receive information and notifications on a screen in the nursing office or tablet devices they can carry on the ward. Staff on the ward can see a clear image of the room for up to 15 seconds only when checking a patient's pulse and breathing rate. They can see an anonymised, blurred image of the room for up to 15 seconds only when a notification has been received to support the completion of an additional safety check.
--	--

Data Privacy Impact Assessment

Benefits:	Improved patient safety and ability to save lives. Ability to be able to undertake important physical observations (life sign measures) without causing additional distress to patient in certain clinical situations.	
Constraints:	Inability to capture who has accessed the system due to lack of individual sign on to use system. Hardware and server administration is provided and managed by third party. Trust infrastructure for WiFi connectivity	
Relationships: (for example, with other Trust's, organisations)	TEWV and Oxehealth, potential to share with coroners, police etc, in line with DPIA and policy, NHS National Forum, Co Creation Group (TEWV, Carers, patients)	
Quality expectations:	Image produced to the expected standard. The physical observations carried out are accurate and align with actual manual physical observations	
Cross reference to other projects:	Oxehealth Pilot – this is the follow on for the continued rollout of the system. Once approved this DPIA will supersede the earlier version.	
Project Manager:	Name:	Dawn Jessop
	Title:	Deputy Chief Nurse
	Department:	Nursing & Governance
	Telephone:	[I/S]
	Email	[I/S]
Information Asset Owner: (All systems/assets must have an Information Asset Owner (IAO). IAO's are normally the Heads of Departments and report to the SIRO)	Name:	Beverley Murphy (Clinical Owner)
	Title:	Chief Nurse
	Department:	Nursing & Governance
	Telephone:	[I/S]
	Email	[I/S]
	Name:	[I/S] (Technical Owner

Data Privacy Impact Assessment

Information Asset Administrator: (All systems / assets must have an Information Asset Administrator (IAA) who reports the IAO as stated above. IAA's are normally System Managers / Project Leads)	Title:	End User Computing Manager
	Department:	Digital and Data
	Telephone:	[I/S]
	Email	[I/S]
Deputy Information Asset Administrator: (It is necessary that there is a deputy in place for when the IAA is absent from the workplace for whatever reason)	Name:	
	Title:	
	Department:	
	Telephone:	
	Email	
Customers and stakeholders: Please list any and all involved including both internal and external parties (ref any project management framework)	Chief Nurse, Deputy Chief Nurse, TEWV Steering Group, TEWV Clinical Subgroup, Oxehealth, Co Creation Subgroup, Patients, Carers/Families	

Section C - Privacy Impact Assessment Key Questions

<u>Question</u>	<u>Response</u>	<u>Ref to key req. e.g. GDPR, DPA18 etc</u>
1. Will the system/project/process (will now be referred to thereafter as 'asset') contain personal identifiable data or special categories (sensitive) data? If answered 'No' you do not need to complete any further information as DPIA is not required.	☐ No Yes ☒ If yes, please specify: ☒ Patient ☒ Staff ☒ Other (specify) Anybody having access to the room	
2. Please state purpose for the collection of the data: e.g. patient treatment, health administration, research, audit, staff administration, service evaluation	VBPMs are assistive tools that enable staff to enhance and support patient safety in inpatient services by delivering noncontact measurement of physiological parameters such as pulse and breathing rate, some degree of patient location, activity or behaviour data and some form of contextual video information (which may be blurred) either in real time or through subsequent reviews. The use of these systems is intended to enhance existing clinical practice and not replace the need for nursing interventions.	Art 5;6;7;8;9;
3. Does the asset involve new privacy-invasive technologies? (e.g. SIRI, Alexa, Smart TVs, bodycameras) (Refer to your risk assessment)	☒ Yes ☐ No If yes, please give details: The Oxehealth Oxevision Vital Signs module requires the display of raw video feed to a user when they seek to take a pulse rate or breathing rate measurement as part of its functionality. This is required to correctly identify the individual being assessed for physical observations.	SS PIA (1)

4. Please tick the data items that are held in the system

Personal }

Special category }

☐ Name	☐ Address
☐ Post Code	☐ Date of Birth
☐ GP	☐ Consultant
☐ Hospital/L A No.	☐ Next of Kin
☐ Sex	☐ ID/NHS Number
☐ Occupation	☐ Local reference number
☐ National Insurance Number	
☐ Contact details	

☐ Political opinion	☐ Sexual orientation/life
☐ Trade union	☐ Religious/Philosophical
☐ Genetic / biometric	☐ Racial / Ethnic Origin
☐ Medical History	☐ Treatment dates/Diagnosis
☐ Criminal offences	

Other (please state here):

PERSONAL DATA

a) Clear Video Data (CVD) – The Oxehealth Vital Signs product module requires the display of raw video feed to a user when they seek to take a pulse rate or breathing rate measurement as part of its functionality. The local secure server also stores encrypted raw video data on a [24 hour] “rolling buffer” for serious incident review or issue resolution, meaning that encrypted video from each room is held securely for [24 hours] after which it is automatically deleted by the software. Video Data which contains images of staff, patients or other personnel is personal data. This is referred to as “Clear Video Data (CVD)”.

Video Data which does not contain images of staff, patients or other personnel is not personal data.

In contrast to Anonymised (blurred) Video Data, Clear Video Data is encrypted but not anonymised because the identifiable data is required fully to investigate the algorithm’s performance (example image, see right). Clear Video Data will be selectively collected in short

	episodes for specific purposes, so the total volume of video will be relatively low. Under certain circumstances Clear Video Data may be “clipped” (marked for retention on the local secure server so that it is not recorded over) by Oxehealth remotely and in some cases securely transferred to Oxehealth’s facilities. The Clear Video Data is stored on a local Tees Esk & Wear Valley (TEWV) secure server for [24 hrs] after which it is deleted and later recorded over making it irrecoverable. Where this data is clipped and saved to the network attached storage for addressing performance issues, it will only be kept for as long as is needed to investigate and resolve the issue. To support this, all data files are date and time stamped so that retention can be tracked. Where this data is clipped and saved to the network attached storage for serious incident review it will be deleted as soon as the data has been transferred to TEWV, and Oxehealth have signed confirmation it has been received. With respect to Clear Video Data collected for addressing performance issues, once the issue for which the data was collected has been addressed, Oxehealth may anonymise the data if it is deemed necessary to retain it to avoid potential performance issues affecting the Oxehealth system in the future. Anonymisation is achieved by applying non-reversible filters over the face and any identifying features of any individuals captured on the video. This is the same filter type used to create Anonymised (blurred) Video Data. This anonymised data is retained by Oxehealth for the purpose of validation and testing of current features and future updates or releases of the Oxehealth System for TEWV, to enable the delivery of the Oxehealth Service to TEWV to the contracted SLA, to ensure that the Oxehealth system is continuously optimised for all TEWV rooms where the system is live, and to avoid potential performance issues affecting the Oxehealth system. Anonymised (blurred) Video Data is no longer personally identifiable data, but it is still owned by TEWV. Oxehealth will retain this data until the end of the contract with TEWV,
--	--

	until it is no longer needed, or until TEWV instructs Oxehealth to delete it, whichever is earlier. Data collected for serious incident review is not retained by Oxehealth but provided directly to the TEWV to support their investigation. Twice per year, Oxehealth provides TEWV with a Video Data Report which details the volume, retention period and retention purpose for any Clear Video Data collected for TEWV for the purposes outlined below. The report will also include whether any Clear Video Data has been anonymised as described above. Oxehealth will process all personal data generated in the project in accordance with this DPIA and documented instructions from TEWV, the Data Controller. As set out above, Clear Video Data may be “clipped” under certain circumstances and in some cases securely transferred to Oxehealth’s facilities. The purpose for which Clear Video Data may be clipped are as follows: 1. Performance Issues: If TEWV identifies a system performance issue with Oxevision or is alerted to a potential performance issue by Oxehealth staff, and the issue cannot be otherwise resolved, TEWV may instruct Oxehealth to clip and review short periods of Clear Video Data in order to investigate and resolve the issue. This may include images of patients if required. Where possible, this video will be anonymised to ensure no data subjects can be identified from the data. In some cases, a performance issue may lead to a “Medical Device Investigation” if it relates to part of the Oxevision product which is a regulated Medical Device (e.g., Vital Signs measurements). 2. Serious Incident Review: Oxehealth may clip Clear Video Data at the request of TEWV senior staff (with Chief Nurse approval) flagging the need to store the Clear Video Data to support an internal or external investigation (for example in which a patient or member of staff was harmed).	
--	--	--

	Where possible, analysis on Clear Video Data for the purposes outlined above will be performed automatically, using computers with processes that do not require a human to view the Data. All TEWV and Oxehealth staff with access to the data are required to be fully trained as to its use, the sensitive nature of this data, and everyone will be required to follow the staff code of conduct. All Oxehealth staff are DBS screened. No Clear Video Data will be used for research, marketing, or publicity purposes. b) Staff Identification Data (SID) The email address of an appointed Tees Esk & Wear Valley manager is recorded as part of site configuration to set a default recipient for report exports. A copy of every exported report (including but not limited to Activity Tracker and Vital Signs Trends reports) is sent to the default recipient so they can audit the distribution of healthcare data within TEWV. Email addresses of all TEWV staff who request a report are also recorded in this way. This data is stored on the local secure server at TEWV, and in Oxehealth's secure cloud services: Gitlab as part of site configuration and AWS for emailing the reports. Staff Identification data stored on the local secure server and on cloud-servers (AWS and Gitlab) for the purpose of providing reports to TEWV is retained until the end of the contract. Oxehealth carries out data accuracy checks on this data with TEWV a minimum of twice yearly to ensure the most up to date data is configured in the system and any data which is no longer correct is deleted. This data can additionally be updated at any time at the request of TEWV Oxehealth process Staff Identification Data when configuring a site to record the email address of an appointed TEWV manager as a default recipient for all export reports in the site config file on Gitlab. In addition, email addresses of all TEWV staff who request a report are stored on the local secure server at TEWV,
--	---

	and in Oxehealth's secure cloud services (AWS) for emailing the reports. Additional processing of staff identification data is carried out by Oxehealth when providing on-boarding, training, and support for the Oxevision service. Staff e-mail addresses will be stored internally (on Forms and IIC) and used for monitoring training on oxehealth to ensure wards meet their required compliance of 85% of staff trained. <u>NON-PERSONAL DATA</u> a) <u>Anonymised (blurred) Video Data (AVD)</u> - Oxehealth will anonymise the camera feed so that the individual is not identifiable from the video. Some modules within the Oxehealth Software permit clinicians to view Anonymised (blurred) Video Data in response to an alert. Oxehealth will also compress and encrypt this feed and transfer it securely to its secure cloud servers. Anonymised (blurred) Video Data is required to ensure the Oxehealth Service delivers the Contract Purpose to the contracted standard. The Anonymised (blurred) Video Data cannot be viewed by unauthorised persons because it is encrypted and – even if it were decrypted - the anonymisation prevents individuals being identified (example, see right). b) <u>Algorithm Processed Data (APD)</u> - These are mathematical results (e.g., wave forms derived from camera pixels) from various processing stages of the algorithms (software calculations measuring movement, for example) including the final log file. Algorithm Processed Data are used in conjunction with the Anonymised (blurred) Video Data to ensure the Oxehealth Service delivers the Contract Purpose to the contracted standard. These data are also encrypted and sent to Oxehealth's secure cloud servers. These data cannot be used to identify an individual. c) <u>User Interface Output Data (UIOD)</u> - When the algorithm has completed its processing of the	
--	---	--

Data Privacy Impact Assessment

	camera feed, saving the information to the log file, it extracts room status reports (known as User Interface Output Data, an example of which would be an alert to an individual getting out of bed, or a vital sign recording was taken) which are supplied to an output server (known as the User Module) so that they can be displayed to TEWV's staff as visual and audible statuses. These User Interface Output Data are recorded by the User Module and drive the audible alerts and screen displays. These data cannot be used to identify an individual. d) Empty Room Video Data (ERVD) – Single frame images of empty rooms that do not contain any personal data (no people or personally identifiable information are visible in the images), are clipped from the raw video feed generated by the Oxehealth Vital Signs product during the install process, and from time to time, to ensure there are no local phenomena which could have a detrimental impact on the services (for example, to verify that there are no unidentified local light effects or that there have been no changes in the room set up or contents that contravene the Software Modules' instructions for use's contraindications, warnings or cautions). Oxehealth can ensure the room is empty and that this data is not personal data using Anonymised (blurred) Video Data and Algorithm Processed Data. Anonymised (blurred) Video Data, Algorithm Processed Data, and User Interface Output Data do not constitute personal data in circumstances where Oxehealth does not have access to Clear Video Data in respect of the same footage. Empty Room Video Data does not constitute personal data in any circumstances.	
5. Will the asset collect new personal data items which have not been collected before?	☒ Yes ☐ No Provide details below: <u>Please refer to section 4 immediately above re Clear Video Data and how it will be handled above.</u>	SS PIA (5)

Data Privacy Impact Assessment

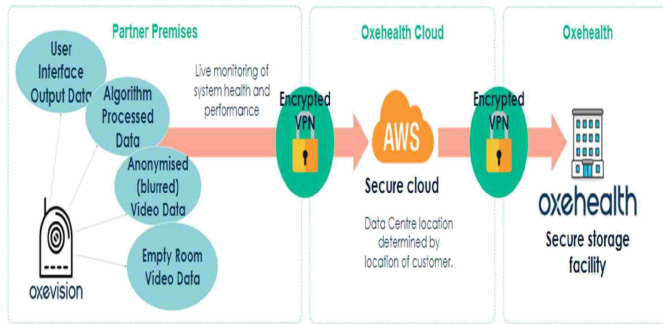
6. What checks have been made regarding the adequacy, proportionality, relevance and necessity for the collection of personal and/or sensitive (special categories) of data for this asset?	☒ Pseudonymisation ☒ Anonymisation ☒ Caldicott checks Provide details below: <u>Please refer to section 4 immediately above re Clear Video Data</u> <i>Caldicott principles will be embedded within the policy development.</i>	SS PIA (2 & 10)
7. Is the third party contract/supplier of the system registered with the Information Commissioner? What is their notification number? Third party must complete the checklist Appendix 1 – Checklist for Third Parties	☒ Yes ☐ No ☐ Not applicable Company name and Data Protection ICO Number: Oxehealth holds ISO/IEC 13485, ISO/IEC 27001 Cyber Essentials Plus certification and is externally audited against these certifications annually. Oxehealth's lead supervisory authority for General Data Protection Regulations is the Information Commissioner's Office (ICO) in the UK and the Swedish Authority for Privacy Protection in Sweden (IMY). Oxehealth has appointed a Data Protection Officer and is registered as a Data Controller with the ICO – registration number ZA065748. Oxehealth complies with the DCB0129 clinical risk management standard and has completed the DAPB0086 Data Security & Protection Toolkit (DSPT) with "standards exceeded".	
8. Who provides the information for the asset? E.g. source of data (ref Information Asset Register IAR/Record of Processing ROP)	☒ Patient ☒ Staff ☒ Others – Please specify 3rd party partner organisation – Oxehealth ROPA Information Asset Register	

Data Privacy Impact Assessment

9. What is the lawful basis for processing Personal Data under General Data Protection Regulation. DPA 2018 (Appendix 2 click) (ref IAR/ROP) NB –DO NOT select 6) (1) a) if processing is for the purpose of direct health or social care	☒ 6) (1) a) Consent - (all article 7 conditions must be met ☐ 6) (1) b) Delivery of a Contract ☐ 6) (1) c) Legal Obligation 6) (1) d) Vital interests ☒ 6) (1) e) A public / official function / Interest	Art 6
10. Does the processing involve special categories of data (ref Question 4)?	☒ Yes ☐ No	
11. If Yes What is the lawful basis for processing Personal Data under General Data Protection Regulation Article 9. (Appendix 2 click) NB –DO NOT select 6) (1) a) if processing is for the purpose of direct health or social care	☒ 9) (2) a) Consent – (all article 7 conditions must be met) ☐ 9) (2) b) Employment, social security etc. ☐ 9) (2) c) Vital interests ☐ 9) (2) d) Legitimate activities (not to be used for public authorities) ☐ 9) (2) e) Data already been made public by subject ☐ 9) (2) f) Legal obligation ☐ 9) (2) g) Public interest ☒ 9) (2) h) Provision of Health or Social Care ☐ 9) (2) i) Public health ☐ 9) (2) j) Historical or scientific research	Art 9
12. Where consent is applied, Please provide details of the consent process and embed any consent forms Note: Consent must follow Article 7 requirements (Appendix 2 – Click)	☐ Explicit consent Provide details below: Patients should always be fully informed about the technology, given details of its use and purpose and details of how to request to “opt out” of its use should they wish. The use of Oxevision must be carefully considered on a case by case, patient by patient basis to ensure that any decision to use such systems has a legitimate aim and is both lawful and fair and safe for the patient.  Consent Flow V8.pdf	Art 7 & 8 & 9

Data Privacy Impact Assessment

13. Please indicate other legislation which provides a legal basis for processing (Please tick relevant legislation or add details as necessary)	☐ Children Act 1989 as amended 2004 ☒ Mental Capacity Act 2005 ☐ Health & Social Care Act 2012 ☐ Care Act 2014 ☐ H&SC (Safe and Quality) Act 2015 ☐ NHS Act 2006 ☒ Human rights Act 1998 ☒ Data Protection Act 2018 Sch 1 para 2 ☒ Other (Please specify) Mental Health Act 1983	
14. If relying on a contract for processing does the third party/supplier contracts contain all the necessary Data Protection clauses including information about Freedom of Information? (check GDPR/DPA2018)	☒ Yes ☐ No Complete Appendix 2 – Third party checklist Provide details below: Please refer to appendix 2	Art 26 Art 28 Art 30
15. Where the Data is being processed, detail where this is recorded / registered.	☒ Information asset register / Record of Processing ☐ Caldicott Approval State where the information above is stored	Art 14
16. How will the data be kept up to date and checked for accuracy and completeness?	Provide details below: With respect to Clear Video Data collected for addressing performance issues, once the issue for which the data was collected has been addressed, Oxehealth may anonymise the data if it is deemed necessary to retain it to avoid potential performance issues affecting the Oxehealth system in the future. Anonymisation is achieved by applying non-reversible filters over the face and any identifying features of any individuals captured on the video. This is the same filter type used to create Anonymised (blurred) Video Data. This anonymised data is retained by Oxehealth for the purpose of validation and testing of current features and future updates or releases of the Oxehealth System for TEWV, to enable the delivery of the Oxehealth Service to TEWV to the contracted SLA, to ensure that the Oxehealth	Art 5 (1) (d)

	system is continuously optimised for all TEWV rooms where the system is live, and to avoid potential performance issues affecting the Oxehealth system. .	
17. Who will have access to/share the information? Ref IAR/ROP (Refer to your stakeholders and relationships lists in Section A)	Include any external organisations. Also how the data will be sent/accessed and secured. Provide details below: Data is collected from every installation of the Oxehealth software in a room. The equipment used to do this is known as a “room installation” with the data stored in a securely encrypted format. This encrypted data is stored on a server which is not in the room but is located nearby on the same site - this is referred to as a “local secure server”. Some of the data collected is stored on secure remote servers provided by Oxehealth’s cloud storage provider Amazon Web Services (AWS) - these are referred to as “cloud servers”. The cloud servers physical location is either in a UK data centre for UK Oxehealth Partners. Figure 1. Non-Personal Data Flows from the Oxehealth Software on Partner premises to Oxehealth:  The diagram illustrates the flow of non-personal data from partner premises to Oxehealth. On the left, under 'Partner Premises', data sources include 'User Interface', 'Output Data', 'Algorithm Processed Data', 'Anonymised (blurred) Video Data', and 'Empty Room Video Data'. These feed into 'Live monitoring of system health and performance'. An 'Encrypted VPN' (represented by a padlock icon) connects this to the 'Oxehealth Cloud' section, which contains 'AWS' and 'Secure cloud' (with a note: 'Data Centre location determined by location of customer'). Another 'Encrypted VPN' connects the cloud to the 'Oxehealth' section, which shows a 'Secure storage facility'. Figure 2. Personal Data Flows from the Oxehealth software on Partner Premises to Oxehealth:	

Data Privacy Impact Assessment

	Data will be collected from every room installation and is transferred, in an encrypted format via Ethernet cabling, to the local secure server, located in a secure TEWV facility. The Oxehealth Software modules hosted on the local secure server are accessed by TEWV staff through fixed monitors located securely on TEWV's premises through a secured, encrypted connection, or through dedicated mobile devices (tablets or phones locked down in kiosk mode) through a secured, encrypted wi-fi connection. In accessing Oxevision, staff interact with various data types including Clear Video Data in their day-to-day use of the system. From the local TEWV based secure server, data travels to Oxehealth via two mediums - over the internet and by the physical movement of storage devices by Oxehealth staff. a) <u>Data that travels to Oxehealth via the Internet (over encrypted connection)</u> Oxehealth will routinely transport Non-Personal Data via the internet. These data allow Oxehealth to monitor and improve the system for the purpose of providing the Oxehealth Service to TEWV as per the defined Service Level Agreements (SLAs) in the Oxehealth Service Agreement. To deliver the service to the contracted standard and to improve the product performance, on occasion, Oxehealth need to obtain an image of a room over the internet via VPN. This is a single frame of an empty room
--	--

	that does not contain any personal data. Prior to transferring the “reference images”, Oxehealth verifies that there is no personal data contained within the images by cross-checking Anonymised (blurred) Video Data and Algorithm Processed Data to ensure no individuals are present. Once this is confirmed, Oxehealth’s internal process requires sign-off from a separate reviewer with specific data protection training before the “reference image” can be transferred. The reference images are transferred to Oxehealth’s secure cloud servers and then to Oxehealth’s secure storage facilities. All data travels using a secure connection (encrypted) from both the on-site local secure server to Oxehealth secure cloud servers, and from the secure cloud servers to secure Oxehealth facilities. b) <u>Data that arrives at Oxehealth via the physical movement of storage devices</u> Clear Video Data is typically too large to transmit via secure internet connection. Instead, this is encrypted and physically transferred on a portable storage device. The storage devices will be exchanged when there is a requirement for Oxehealth to retrieve Clear Video Data for (1) addressing performance Issues, or (2) for serious incident review, with the devices physically being transferred to Oxehealth’s secure data storage facility. During this transfer process Oxehealth will accompany the storage devices at all times. Once in the secure data storage facility, the data will be transferred onto medium term storage located in a secure server room. Once the transfer is complete, deletion utilities are run to ensure the data can no longer be accessed on the storage device. From Oxehealth data is transferred to TEWV via secure email (Egress) utilising DocuSign for authorisation. c) <u>Data that is transferred to TEWV via the physical movement of storage devices</u> If Clear Video Data has been extracted to support a TEWV investigation, the Clear Video Data clip will be delivered to a named TEWV recipient as stated by one of the four named TEWV authorisers (Chief Nurse, Deputy Chief Nurse, or one of the two Directors of Nursing Quality) when using DocuSign to authorise the retrieval. The CVD is then stored on a restricted access shared	
--	--	--

Data Privacy Impact Assessment

	drive on the Trust network by the Trust's authorised recipient.. The processing of this data by TEWV staff will follow the VBPMs Oxevision policy regarding the secure storage and logging of access to view the video footage.	
18. Do you intend sending direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?	☐ Yes ☒ No If yes, have you obtained consent? Provide details below:	Privacy Check
19. If answered Yes to Q18 – Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulations 2003 (Appendix 2 click)	☐ Yes ☐ No ☒ Not applicable If yes provide details below:	Privacy Law Check
20. If applicable, are there procedures in place for an individual's request to prevent processing for purposes of direct marketing in place?	☐ Yes ☐ No ☒ Not applicable	Privacy Check
21. Is automated decision making used? If yes, how do you notify the individual? Can there be any human intervention if required?	☐ Yes ☒ No Provide details: ☐ Yes ☐ No	Privacy Check Art 22
22. Is there a useable audit trail in place for the asset? For example to identify who has accessed a record.	☒ Yes ☐ No	DSPT
23. Can the data be easily obtained by the data Subject upon request?	☒ Yes ☐ No	Art 15
24. Have you assessed that the processing of personal / special categories of data will not cause any unwarranted harm to the	☒ Yes ☐ No Embed risk assessment if separate document	Art??

rights and freedoms of the individuals concerned? What risk assessment has been carried out? (Appendix 3 click)	Data generated by the Oxevision system will be stored on the local compute equipment securely at TEWV while it is being recorded. (local secure server and network attached storage). In these storage locations, Personally Identifiable Data (Clear Video Data and Staff Identification Data) will be encrypted at rest to the AES256 standard. All data transmission between local compute equipment at TEWV 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. Each member of Oxehealth staff which has access to provide support for the Oxevision system at TEWV site, uses a unique set of credentials for Virtual Private Network (VPN), remote machine access and file server access. Staff VPN access is granted to selected staff and is audited. Logging and pattern-based alerts are active on the firewall and VPN. Any data transfer over the internet will use SSL encryption to the AES256 standard. All data stored on Oxehealth's Secure Cloud Servers will be encrypted at rest to the AES256 standard. Where the transfer of Clear Video Data to Oxehealth's secure facility is required, the data will be encrypted to AES 256 standard and stored on a password protected network attached storage device (NAS). The NAS will be transported to Oxehealth's office by a member of the Oxehealth team. The data will then be transferred from the NAS to Oxehealth's storage servers. These are located within a secure UK facility that has strict access controls. All server room physical access and file electronic access are logged and audited. The facility is within an alarmed building which has 24-hour security guards.	
--	---	--

Data Privacy Impact Assessment

	Access to data on Oxehealth secure servers is limited to a small number of approved members of the team as required to perform a specific task, with fine grained access control on data permissions managed through active directory and audited quarterly. Oxehealth has implemented an Information Security Management System (ISMS) for assessing and managing security technology and policies to ensure measured protection of all assets (including TEWV information assets). In addition to strong physical security, the Oxehealth network also has a high level of electronic security to minimise the likelihood of a network-based attack. The Oxehealth network is protected with a perimeter Unified Threat Management (UTM) firewall, scanning and protecting the gateway from external threats (including intrusion prevention, anti-virus, anti-spyware and botnets). Oxehealth facility infrastructure and the Oxehealth software service and provided hardware infrastructure are subject to regular penetration testing and cyber security vulnerability testing using CREST certified external auditors.	
25. Do you have a compliant privacy Notice	☒ Yes ☐ No If yes Embed here Privacy notices - Tees Esk and Wear Valley NHS Foundation Trust (tevv.nhs.uk)	Art 19
26. What are the retention periods for this data? (please refer to the NHS Code of Practice Records Management)	Will be retained in line with the NHS Code of practice records management (2021) – otherwise as detailed below <u>Non-Personal Data</u> a) The Anonymised (blurred) Video Data, User Interface Output Data and Algorithm Processed Data are stored in Oxehealth's secure cloud servers, provided by Amazon Web Services. Oxehealth has a retention policy of 2 years for	SS PIA (13)

	these data, after which they will be deleted. They may be deleted sooner when requested by a Partner, at the end of the contract or when no longer required to support system performance b) The Empty Room Video Data is stored in secure servers at Oxehealth's premises and as part of TEWV site configuration data in Gitlab. Where it is stored on Oxehealth's server it may be kept for the lifetime of the system, otherwise it will be deleted at the end of the contract, or when no longer needed to support system performance. <u>Personal Data</u> a) <u>Clear Video Data</u> The Clear Video Data is stored on the local secure server for 24 hrs after which it is deleted and later recorded over making it irrecoverable. Where this data is clipped and saved to the network attached storage for addressing performance issues, it will only be kept for as long as is needed to investigate and resolve the issue. To support this, all data files are date and time stamped so that retention can be tracked. Where this data is clipped and saved to the network attached storage for serious incident review it will be deleted as soon as the data has been transferred to TEWV, and we have signed confirmation it has been received. With respect to Clear Video Data collected for addressing performance issues, once the issue for which the data was collected has been addressed, Oxehealth may anonymise the data if it is deemed necessary to retain it to avoid potential performance issues affecting the Oxehealth system in the future. Anonymisation is achieved by applying non-reversible filters over the face and any identifying features of any individuals captured on the video. This is the same filter type used to create Anonymised (blurred) Video Data. This anonymised data will be retained for the purpose of validation and testing of current features and future updates or releases of the Oxehealth System for TEWV, to enable the delivery of the Oxehealth Service to TEWV to the contracted SLA, to ensure
--	---

	that the Oxehealth system is continuously optimised for all TEWV rooms where the system is live, and to avoid potential performance issues affecting the Oxehealth system. Anonymised (blurred) Video Data is no longer personally identifiable data, but it is still owned by TEWV. Oxehealth will retain this data until the end of the contract with TEWV, until it is no longer needed, or until TEWV instructs Oxehealth to delete it, whichever is earlier. Data collected for serious incident review is not retained by Oxehealth but provided directly to the TEWV to support their investigation. Twice per year, Oxehealth provides TEWV with a Video Data Report which details the volume, retention period and retention purpose for any Clear Video Data collected for TEWV. The report will also include whether any Clear Video Data has been anonymised as described above. Oxehealth will process all personal data generated in the project in accordance with this DPIA and documented instructions from TEWV, the Data Controller. In order to support communication on the ward regarding the Oxehealth software, templates for ward signage and information leaflets can be provided by Oxehealth on request. b) <u>Staff Identification Data</u> Staff Identification data stored on the local secure server and on cloud-servers (AWS and Gitlab) for the purpose of providing reports to TEWV is retained until the end of the contract. Oxehealth carries out data accuracy checks on this data with its Partners a minimum of twice yearly to ensure the most up to date data is configured in the system and any data which is no longer correct is deleted. This data can additionally be updated at any time at the request of TEWV	
27. How will the data be destroyed when it is no longer required?	Provide details below: <i>Please see section 26 above</i>	IGTK

Data Privacy Impact Assessment

28. Does the asset involve new linkage of personal data with data in other collections, or are there significant changes in data linkages?	☐ Yes ☒ No If yes provide details below:	SS PIA (8)
29. Where will the data be kept/stored/accessed?	☐ On paper ☒ On a database saved on a network folder/drive ☐ Website ☒ On a dedicated system saved to the network ☐ Other – please state below:	Art 5(f) €
30. Will any data be transferred outside the organisation premises or systems? If 'Yes' where is this information being sent	☒ Yes ☐ No Please provide details: In the event of requiring review by legitimate 3 rd parties, e.g., coroner enquiry	IGTK 208 & 308
31. Please state by which method the data will be transported.	☐ non secure Email ☒ Secure Email ☐ Website ☐ courier ☐ By hand ☐ post – internal ☐ telephone ☐ post – external ☐ Secure File Transfer ☐ Other – please state below:	IGTK 208 & 308
32. What level of encryption is being used where transfer is electronic?	SSL encryption AE256 standard is employed for all interfaces:	
33. Are you transferring any personal and / or sensitive data to a country outside of the UK? Please name the country Does this include back-up arrangements?	☐ Yes –Within the European Economic Area (EEA) ☐ Yes –Outside the European Economic Area (international) ☒ No Provide details below N/A	IGTK 209 Art 5(f) Art 44 / 45

Data Privacy Impact Assessment

34. If transfer is outside of the EEA, what measures are in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country? (DPO to assess ICO decision for bulk transfers)	Please provide details: N/A	IGTK 209 Art 35(PIA) Art 32 Art 44 / 45 / 46
35. All transfers outside of the UK <u>must</u> be approved by the organisation Data Protection Officer (DPO) Please provide DPO documented approval	Please provide details: N/A	
36. Is there a Security Management Policy and Access Policy in place? Please state policy titles.	☒ Yes ☐ No Access to Information Systems Policy https://intranet.tevv.nhs.uk/download.cfm?doc=docm93jjm4n1803.pdf&ver=16395 Information Security and Risk Policy https://intranet.tevv.nhs.uk/download.cfm?doc=docm93jjm4n1152.pdf&ver=18382	SS PIA (11)
37. Is the Processor compliant with the 10 data and cyber security standards – the '17/18 Data Security Protection Requirements' (2017/18 DSPR)	☒ ISO/IEC 27001:2013 ☐ Cyber Essentials (CE) certification ☒ Cyber Essentials Plus (CE+) certification ☐ Digital Marketplace ☐ Other (please state) N/A Evidence provided: ☒ Yes ☐ No	
38. Has an information risk assessment been carried out and reported to the Information Asset Owner (IAO)?	☒ Yes ☐ No Please provide details below as to how the risks will be managed and mitigated (include any inclusion of relevant risk register) see section D	Risk Ass
39. Is there a contingency plan / backup policy in place to manage the effect of an	☒ Yes ☐ No	Risk Ass Art 33 / 34

Data Privacy Impact Assessment

unforeseen event? Please provide a copy.	In the event of any system outage, all staff on the ward must be informed immediately. Staff will then continue to perform all safety and care requirements without the use of Oxevision, and update care documents and risk assessments as required dependent upon length of period of system outage. This statement is contained within the VBPMS Oxevision Policy	
40. Are there procedures in place to recover data (both electronic /paper) which may be damaged through: • Human error • Computer virus • Network failure • Theft • Fire • Flood • Other disaster	☒ Yes ☐ No Data on the local Oxehhealth servers capture the 24 hour CVD data. This is not recoverable data. Copies of clipped CVD data held on Trust network shared drives will follow Trust policy and procedure for back up in the event of damage listed. If yes provide details and procedure / policy titles below:  TEWV Backup regime -Server Backup Inform	Risk Ass

Section D – Risk Assessment

Impact: 1 = Negligible, 2 = Minor, 3 = Moderate, 4 = Major, 5 = Catastrophic

Likelihood: 1 = Rare, 2 = Unlikely, 3 = Possible, 4 = Likely, 5 = Almost certain

Exposure = Impact x Likelihood

See Appendix 3 for examples of possible risks.

Risk description	Inherent Privacy Risk			*Options for avoiding or mitigating this risk	Residual Privacy Risk		
	Impact	Likelihood	Exposure		Impact	Likelihood	Exposure
Power Loss	3	1	3	Follow Business Continuity Protocols for power outage within the Trust. Regarding Oxevision VBPMS - normal procedures and process for observation and engagement will be maintained as per normal. Oxehealth isn't envisaged to take the place of staff therefore BAU as per the SOPs will be in place	3	1	3
Audit trail does not identify staff accessing the system but does capture date and time of access.	3	5	15	It is not currently possible to identify which members of staff accessing the system and when. The closest we can reliably understand this is on a shift by shift basis when consulting the health roster to identify who was on shift On discussion with Oxehealth the system does not currently support individual PIN access, but they are currently seeking to develop this	Current risk score 4 Future score 3	Current risk score 3 Future score 3	Current risk score 12 Future score 9

Data Privacy Impact Assessment

				functionality as it has also been discussed with other Trusts. There is no specific timeline identified for this functionality to be implemented at present - it remains in the design stage. Future developments include: Oxehealth are currently working on a more detailed approach to audit logs due to national demand – timeframe remains unclear at present. TEWV currently exploring the use to individual logins for staff using the VBPMS			
Service users not being appropriately informed of the Trust's processing activity.	4	4	16	Action plan derived from service evaluation and development of policy and SOP together with training plan, and the development of cocreated (with patient and carers) information leaflets will support in addressing this issue. This requirement is clearly laid out in the SOP for all staff to follow, the advent of improved training packages (see below) to provide a more consistent and standardised approach across the Trust and will contribute in achieving the mitigation of this risk. These documents were be made available for Trust wide consultation w/c 01/04/24 with the view that the fundamental approaches will not have	4	2	8

Data Privacy Impact Assessment

				any significant changes applied. Additionally, this is reinforced via the fortnightly held clinical subgroup. An audit tool and checklist are currently in development to support oversight an monitoring regarding this			
Staff misunderstand the purpose and use of the system	3	3	9	Action plan derived from service evaluation and development of policy and SOP together with training plan, and the development of cocreated (with patient and carers) information leaflets will support in addressing this issue. Currently progressing how Oxevision training is included in Statutory and Mandatory training for all inpatient staff (including bank staff - will need to consider this requirement regarding Agency staff). This will have an 85% KPI requirement. Use of revised training package provided by Oxehealth regarding how to use the system, and current considerations towards building a Trust bespoke package regarding a contextual approach to the use of Oxehealth regarding, consent, data protection, and privacy.	3	2	6

Data Privacy Impact Assessment

Data disclosed inadvertently to a third party or data is lost. The video data could become public. A breach of the patient's privacy and confidentiality, if information about their treatment is made known to third parties. This could cause distress to the patients.	4	3	12	The local secure server will be located at TEWV, and should be provided with appropriate physical and electronic access restricted to authorised TEWV or Oxehealth personnel by TEWV. 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 TEWV 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 a number of 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 TEWV • Portable storage devices are always accompanied in transit by Oxehealth staff	4	2	8
---	---	---	----	---	---	---	---

Data Privacy Impact Assessment

				• 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 • Clear 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		
--	--	--	--	--	--	--

Data Privacy Impact Assessment

				and personally identifiable data collection is kept to a minimum only where necessary to provide the service to the contracted standard. All TEWV staff to maintain compliance with detail and accommodations made within the policy to address secure storage of any “clipped data” which any stored data will be audited for compliance to DPA 2018.			
Unnecessary intrusion into a patient's privacy. Ongoing monitoring is more invasive to privacy rights than ‘spot-checks’ via staff, and potentially involves more third parties seeing the patient alone in their room. This could cause distress to the patients.	3	4	12	As identified above within this assessment, the nature of this project means that video recording of patients is undertaken.. The Oxehealth Software does not function as a video surveillance system – it is not possible for clinicians to view a continuous feed of clear video data as they would with CCTV. The video is processed by algorithms which then deliver alerts to display units, the goal of which is to improve the current patient safety and care regimes of TEWV. Clinicians are required to view short bursts (maximum of 15 seconds) of video when they use the ‘Take Vitals’ module to ensure they take breathing and pulse rate measurements accurately.	2	3	6

Data Privacy Impact Assessment

				Clear Video Data is occasionally needed to ensure the service is delivered to the contracted standard. The use of Clear Video Data is kept to a minimum, used only in accordance with the purposes highlighted above and in the policy, all of which involve very short, isolated periods that occur: (1) on an occasional, non-routine basis to address performance issues under instruction from TEWV or (2) to provide data to support TEWV, with a serious incident review. All other patient data collected and generated by the Oxehealth system is anonymised and, where Oxehealth staff do not have access to other data which would help them to identify the individual, is not personal data .			
Identification of a patient by an Oxehealth staff member (i.e. if the patient is known personally to the staff member). People external to TEWV become aware of a patient's use of a room. The Oxehealth staff member could tell other people known to the data subject. This could cause distress to the patients.	3	2	6	There is a low risk of Oxehealth staff being able to identify patients from Clear Video Data, given the limited number of Oxehealth people able to review this Clear Video Data, the use of automated processing by computer, and the infrequency of this processing task. The risk of identification cannot be ruled out but is considered to be very low – in addition, Oxehealth staff are bound by its detailed code of conduct concerning the use and security of patient data.	3	1	3

Data Privacy Impact Assessment

				In the event of a member of the Oxehealth team being able to identify a patient involved in the project, Oxehealth will consult TEWV; the default action is to delete all data relating to that patient but TEWV may instruct Oxehealth to pursue another course of action (for example, preserving the data for the purpose of an internal or external investigation).			
Data retained longer than necessary Data pertaining to a patient is retained longer than required, increasing the security risk and risk of a breach of confidentiality.	2	3	6	In the project, TEWV is the data controller and Oxehealth is the data processor. As such, Oxehealth will process all personal data generated in the project in accordance with documented instructions from TEWV (unless applicable law prevents Oxehealth from doing so). Clear Video Data is stored on the local secure server at TEWV site for 24hrs and is then automatically deleted. Where Clear Video Data is clipped and saved to the NAS it will only be kept for as long as is needed to address performance issues raised by TEWV staff or by engineers at Oxehealth on instruction from TEWV, after which it will be securely deleted. If it is deemed necessary to keep data for longer for regression testing of future releases, the data will be anonymised so it is no longer personally identifiable data.	2	2	4

Data Privacy Impact Assessment

				To support this, 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 TEWV with a Video Data Report which confirms the purpose, principles and review process for any Clear Video Data collected for TEWV and a log of the personal data retained, reasons for retentions and date of next review. The report will also include whether any Clear Video Data has been anonymised and retained for future testing. Staff Identification Data recorded in the site repository for the purpose of delivering reports will be kept until the end of the contract with TEWV and will be deleted when TEWV stops using the service. Bi-annual checks will be carried out to ensure this data is accurate and data is deleted for staff who are no longer with TEWV Detailed information on data usage and retention. Is describe above.			
Patient unaware their data is being collected	3	3	9	Patients in the proposed rooms of TEWV are in the care of expert and highly	3	2	6

Data Privacy Impact Assessment

The patient is unaware of their rights under the General Data Protection Regulations (GDPR), and therefore unable to exercise them				trained TEWV staff who will take decisions in the best interest of those patients. TEWV will maintain a regime that informs patients in an appropriate fashion in accordance with policy and procedure to ensure transparent communications have been undertaken to the patients, carers and families at each opportunity as required (i.e. determined by mental capacity and current mental health of the patient). Policy and procedure are currently under development and will be made available when out for Trust wide consultation 22 Feb 2024 with the view that barring minor changes they will fundamentally support in mitigating the risk identified. Additionally, this is reinforced via the fortnightly held clinical subgroup.			
Personal data is accidentally shared with Oxehealth Personal data pertaining to a patient is processed by Oxehealth in systems not designed for personal data storage and processing, increasing the security risk	3	3	9	Patients in the proposed rooms of TEWV are in the care of expert and highly trained TEWV staff who will take decisions in the best interest of those patients and share only appropriate data with Oxehealth when providing feedback through the Oxehealth software forms and through email communication with Oxehealth customer support.	3	2	6

Data Privacy Impact Assessment

and risk of a breach of confidentiality.				Oxehealth provides on-screen warnings to staff to avoid personal data on all Oxehealth software functions where data may be accidentally shared, and further train staff on the use of the software as part of the service. Oxehealth has further implemented a redaction process within its customer support process, to ensure that any personal data accidentally shared is removed from all Oxehealth records, and not further processed by Oxehealth.			
Data moved to another country with different data protection rules Reduced protection on rights and freedoms of data subjects.	3	2	6	All data generated by the Oxevision system is stored on local secure servers at TEWV site. Some data (AVD, APD, UIOD, and SID) is additionally backed up to Oxehealth's secure cloud servers provided by Amazon Web Services. The physical location of the cloud server is in a UK data centre for UK Partners. Where Oxehealth is instructed to transfer Clear Video Data from an overseas territory to Oxehealth's secure servers in the UK to investigate a potential issue with the system which they have been unable to resolve with anonymised data, the European Commission's adequacy decision for data transfers to the UK under the EU GDPR says that the UK provides adequate protection for	3	1	3

Data Privacy Impact Assessment

				personal data transferred from the EU to the UK under the EU GDPR. Oxehealth may process a small amount of Staff Identification Data (name and email address) through international software providers with servers outside of the EU, UK and US. Where this happens Oxehealth will ensure contractual agreements with these providers include appropriate safeguarding measures such as corporate binding rules or standard contractual clauses, and will notify TEWV of these providers.			
The legal basis for the sharing of data and the use of consent within the trust is not clear	4	4	16	Patients should always be fully informed about the technology, given details of its use and purpose and details of how to request to "opt out" of its use should they wish. The use of Oxevision must be carefully considered on a case by case, patient by patient basis to ensure that any decision to use such systems has a legitimate aim and is both lawful and fair and safe for the patient. It is noted that the Trust underwent a cocreated approach to the development of the VBPMs policy which considered any changes to this approach to the consent	2	3	6

Data Privacy Impact Assessment

				model, which at the appropriate time of ratification will be reflected in the standard operating procedure. Both documents have been consulted on Further information and recommendations from NHSE, who are convening a national forum to discuss VBPMS in mental health and Learning Disability services also provided further guidance and/or mandated approaches which influenced the final approach adopted by the Trust when these are published. The current operation model requires that: • All service users will be informed prior to and upon admission that Oxevision is in use on the ward. • For the first 72 hours of admission to support patient safety on the ward, all service users will have the VBPMS switched on. They will be informed of how to request to opt out should they wish to do so. ○ Within the initial 72 hours on the ward the MDT will make a clinical			
--	--	--	--	--	--	--	--

Data Privacy Impact Assessment

				decision recommending that the VBPMS be switched off or on for the individual patient., based upon a balanced view of: ▪ Risk ▪ Recognition of any potential harms to patient from the use of VBPMS ▪ Consideration of alternative approaches and interventions ▪ Patient choice ▪ Best interests of the patient ○ Based upon these same criteria listed above, after the initial 72 hour review the following trigger events will initiate further reviews of the required status of the VBPMS (i.e., whether it is “switched on” or “switched off”): ▪ At each patient’s regular MDT			
--	--	--	--	--	--	--	--

Data Privacy Impact Assessment

				meeting. ▪ When there is a change in risk that will impact upon the required VBPMS status to support patient safety. ▪ A change in the patient's mental capacity ▪ A change in the potential harms to the patient by the VBPMS ▪ The patient chooses to opt out of using the VBPMS. • Service users and carers must be informed and told of the use of VBPMS including the use of video data, both on admission and throughout their stay in hospital. • Service users can raise questions and concerns, and there should be regular opportunities for service users to be engaged by staff in conversation about their			
--	--	--	--	--	--	--	--

Data Privacy Impact Assessment

				questions and concerns. • The service user can request to opt out at any time. • Any request to opt out by a service user should be discussed with the multi-disciplinary team at the next available and appropriate opportunity, and with the service user, carers, family, and advocate (where practicable). ○ Where it is assessed that the service user lacks capacity regarding consent all decisions should take place within the guidance of the best interest process (MCA 2005). This would facilitate personalised consideration of individual preference, safety/risk, and other alternatives. This <u>MUST</u> be documented within the patient's notes within the electronic patient record system, alongside an updated safety summary. ○ Patient advocacy should			
--	--	--	--	--	--	--	--

Data Privacy Impact Assessment

				also be taken into consideration for any decisions, which must be clearly documented within the electronic patient record. It is the responsibility of the ward team to ensure that the status for each room within the ward that's use Oxevision (i.e., whether it is "switched on" or "switched off") is reviewed on a daily basis within the daily report out or other daily review process. Further information and recommendations from NHSE, who are convening a national forum to discuss VBPMS in mental health and Learning Disability services will also provide further guidance and/or mandated approaches which will further influence the final approach adopted by the Trust when these are published.			
The recordings and management of the information gathered is not recorded properly on IAR.	4	4	16	The process of acquiring "clipped" video footage from the VBMS via Oxehealth requires final approval from the Chief Nurse or Deputy Chief Nurse or	4	1	4

Data Privacy Impact Assessment

				Directors of Nursing and Quality. The responsibility and the management of these data will reside with Nursing & Governance who will follow the requirements detailed in the policy.			
The handling of data provided by Oxehealth in the form of encrypted data sticks and its onward usage is yet to be documented	4	4	16	The process of acquiring "clipped" video footage from the VBMS via Oxehealth requires final approval from the Chief Nurse or Deputy Chief Nurse or Directors of Nursing and Quality. The responsibility and the management of these data will reside with Nursing & Governance who will follow the requirements detailed in the policy.	4	1	4
Privacy Notice doesn't advise that VBPMS is used in our facilities and there is no signage advising of its use on the wards.	3	5	15	The Trust has patient information leaflets which are provided to patients alongside discussing the use of VBPMS on the ward. There are ward posters which also highlight that VBPMS is on the ward. It is the responsibility of the ward manager with oversight from the matron to ensure that these remain on display and are visible upon entry to the ward before arriving at the bedroom / seclusion room areas. The privacy is currently being progressed to regarding an update that VBPMS are being used within the Trust	3	2	6

Data Privacy Impact Assessment

				inpatient areas similarly to that of body cameras, however the overarching principles of the privacy notice regarding the protection of privacy and confidentiality remain applicable in regard to the use of VBPMS.			
--	--	--	--	--	--	--	--

Section E - Sign off, actions and outcomes

*******Information Governance To Complete*******

DPIA Reviewed by	[I/S] Information Compliance Manager	Review Date	July 2025
IT Service Desk Reference:		DPIA Central Register Reference	065

Summary of IG Advice:

Ongoing support and challenge offered.

Clarity requested as to some of the mitigations:

- Are patient leaflets in place now - can I view it please
- Are posters on display in wards now?
- How far away are the SOPs in terms of development ?
- Is staff training available now?
- I appreciate that the policy is still in draft – is there a date for consultation – ratification etc

To be presented to IGG 20/12/23 – 21/02/24 - 17/01/24 please see minutes for details of discussion if required. Approval to continue to roll out not given on each occasion. Outstanding issues:

- Consent model
- Policy and Procedures for use not in place / agreed
- How video recordings will be managed and shared from the supplier if required or requested.

15/03/24 Discussion with JB and Updates.

- There is an Options paper being presented to Exec (EDG on the 2nd April 2024. This has been pulled together taking on board comments from IG representatives the Human Rights Council and information gathered as part of the co creation groups. There will be four options:
 1. Implicit Consent Model
 2. On at admission for 72 hrs and then review any concerns and objections based on patient dialogue (Human Rights Council – definitely not in favour of this option)
 3. Assessment at the point of admission once patient on the ward
 4. Assessment prior to admission via the Crisis Teams

It is anticipated that option 3 will be favoured.

- The Policies and Procedures will be updated to reflect the agreed option after the meeting and then put out to consultation that week (w/c 1st April 2024) Consultation will be 6 wks, then it will need to be shared with Clinical Groups and Management and so may not be concluded until June time
- Exec (EDG on the 2nd April) will also be asked to agreed that the draft policy and draft procedure can be implement with immediate effect subject to any revisions following consultation. This ask is in lieu of the fact that it has been identified that current policy and procedures are not at the standard that the Trusts requires to manage the oxehealth safely.

Data Privacy Impact Assessment

The information populated above will be presented to IGG on the 20th March 2024. The ask of IGG is to accept the way forward as agreed by Exec EDG on the 2nd April 2024. The DPIA will then be updated to reflect these agreements and brought back to IGG on 17th April 2024 for final sign off.

There is a request that it is confirmed by IGG that these actions and undertakings will satisfy the issues raised by IGG and the roll-out to additional wards can be undertaken.

IGG decision 22/3/24:

There was a real positive discussion about the work which is ongoing however until the Exec Group on the 2nd have agreed the way of working as per the options paper and have agreed to accept the WIP Policy and Procedure for use until the consultation and ratification happens during the summer it was felt that approval for the DPIA could not be granted.

The group requested that I advise you that the next IGG is the 17th April and papers should be provided by the 5th April. It was felt that if the DPIA could be refreshed and updated to include the decisions made at Exec on 2nd then the mitigations which are supported by the policy and procedures could be accepted. Further more the 'consent' element depending on the preferred option could be if appropriate properly addressed in the risk section.

Action Assigned	Responsibility	Due	Completed
Click here to enter text.	[I/S]	asap	10/07/2024
Risk Mitigations approved by: <i>(a person of seniority on the project)</i>	Click here to enter text.		Click here to enter text.
Remaining Risks accepted by: <i>(a person of seniority on the project)</i>	Click here to enter text.		Click here to enter text.
Can the DPIA be passed to Data Protection Officer for Approval?	☐ Yes ☐ No		Click here to enter text.

Data Privacy Impact Assessment

DPO Advice Provided	☐ YES	Date	
Summary of DPO advice: N/A			
DPO advice accepted	☐ YES ☐ NO	NB: If no state reason why below	
Comments: N/A			
Residual High risk	☐ YES ☒ NO	(if yes report to ICO)	
ICO Outcome: N/A			
DPIA Approved ☒ YES ☐ NO DATE: Information Governance Group 17 July 2024 If no please justify			
DPIA Review Due Date	31 July 2025	DPIA Owner	Joe Bergin

NB- Under Current Data Protection legislation DPIAs must be approved by organisation's Data Protection Officer (DPO)

Appendix 1 – Checklist for Third Parties

Third Party Details:	
Third Party Name:	Oxehealth Limited, Registered in England and Wales, Company Registration Number 08163325
Address:	Magdalen Centre North, The Oxford Science Park, Littlemore, North OX4 4GA
Contact No.	Click here to enter text.
Name of Key contact:	Click here to enter text.
Contact details of key contact:	Click here to enter text.
Data Protection Notification No. <i>(if registered with the ICO)</i>	ZA065748
Please describe the service that is being supplied:	Oxehealth is a spinout from the University of Oxford Institute of Biomedical Engineering and a global leader in vision-based patient monitoring – dedicated to helping mental health clinicians deliver safer, higher-quality and more efficient inpatient care. As members of the NHS Confederation, Oxehealth partners with half of NHS England's mental health providers and is beginning to transform inpatient care in Europe and the US. Oxevision was co-produced with patients, carers and clinicians and is the only patient monitor designed for mental health. To date, it has supported over 30 million hours of patient care. Oxevision enables staff to: visually confirm a resting or sleeping patient is safe without entering their room and disturbing them; measure a patient's pulse and breathing rate remotely; and document therapeutically valuable digital observations. It also generates alerts and reports that help staff know when to intervene proactively and enable them to plan person-centred care.

Data Protection Checklist:		
1	What data are you processing on our behalf?	Data is generated and processed automatically by the Oxevision system and is then additionally processed by the system users (customer staff) and by Oxehealth as follows: Clear Video Data (CVD) – The raw video footage or still images (may contain images of staff, patients or other people (PII) or may

	contain empty room images captured by automatic operation of Oxevision is processed: • automatically by the software installed on servers at customer sites to generate the vital signs measurements and movement alerts and stored on the local secure server for up to 24hrs before being automatically deleted. • By system users (customer staff) who view up to 15 seconds when taking vital signs measurements to confirm they are accurately taken from the correct individual or when reviewing Clear Video Data which has been clipped to support a serious incident review. • By Oxehealth UK technical staff at the request of the customer to save specific clips of data for longer than 24hrs and deliver it to customer staff for serious incident review, or to resolve a complex issue with the medical device software. • Where Clear Video Data is provided to customer staff for Serious Incident Review if this provision is via Egress Secure Workspace then the data will be stored on Egress secure servers in the UK for up to 30 days before being automatically deleted. Anonymised (blurred) video data (AVD) - Created by irreversibly blurring the visual data feed from the camera. Individuals cannot be identified from this data alone and all stored data is pseudonymised. • Automatically generated by the software and stored on the local secure server at customer site before being uploaded via secure SSL connection to Oxehealth's AWS UK secure storage. • Processed by Oxehealth UK technical staff to support initial system configuration (blind running), provide standard maintenance (monitor performance and address issues) and Improve the performance of the product in use by the customer and ensure there
--	--

	is no negative impact from any changes made. Interface Output Data (UIOD) – Room status reports extracted by the algorithm, once it has completed it's processing of the camera feed. Individuals cannot be identified from this data alone and all stored data is pseudonymised. • Automatically generated by the software and delivered to the system users (customer staff) via tablets or static screen in the nurses station in the form of audible alerts and screen displays and stored on the local secure server at customer site before being uploaded via secure SSL connection to Oxehealth's AWS UK secure storage. • Processed by Oxehealth's UK technical team to restore the service in the event of failure or disaster scenario and for usage and performance monitoring. Algorithm Processed Data (APD) – Mathematical results from various processing stages of the algorithms (e.g. software calculations measuring movement), including vital signs measurements. Individuals cannot be identified from this data alone and all stored data is pseudonymised. • Automatically generated by the algorithms when processing the camera feed and stored on the local secure server at customer site before being uploaded via secure SSL connection to Oxehealth's AWS UK secure storage. • Processed by the Oxehealth technical team to support initial configuration of the software (blind running), provide standard maintenance (monitor performance and address issues), and improve the performance of the product in use by the customer and ensure there is no negative impact from any changes made. Empty Room Video Data (ERVD) – Single frame images of empty rooms clipped from
--	---

	clear video data that do not contain any personal data. • Transferred to Oxehealth secure servers in the UK and processed by the Oxehealth UK technical team to configure the software for the specific room as part of the installation process or where the view of the room significantly changes – e.g. due to a camera slip. • Viewed by the Oxehealth UK technical team to check for local phenomenon in the room which could have a detrimental impact on the services. System Performance Data (SPD) – Metrics for monitoring system level hardware and software component health. 1. Automatically generated by Oxevision to deliver the service to the contracted standard and stored on the local secure server at customer site before being uploaded to AWS UK secure storage. 2. Processed by the Oxehealth UK technical team to remotely monitor the performance and connectivity of the system. Oxehealth teams in the UK also processes the following customer staff data to provide the service to its customers as follows: • Personal information (such as name, work address, work phone and email contact information, customer reference id, job role and place of work) • Other information we collect for the processing purpose may include customer reference ID, organisation bank account details, signatures, meeting minutes and debrief notes, ward names, site plans, site details, nature and details of feedback responses or support requests including date & time. The usage of all data generated by the Oxevision system is outlined in more detail in
--	---

Data Privacy Impact Assessment

		the Oxevision DPIA and is governed by the generated data guide which forms part of the service agreement signed with customers. Further information on the processing of customer staff data is available in Oxehealth's customer privacy notice .
2	Where will you be processing the data? Detail sites	Processing of data is detailed in 1 above. Data stored on Oxehealth's AWS storage is stored in a UK data centre. Data stored on Egress storage is stored in a UK data centre (provided by AWS or Microsoft Azure) If data is transferred to Oxehealth's internal secure storage, this will be local storage at Oxehealth's Magdalen Centre North office
3	Will your staff have remote access to the NHS / LA data? If so, please explain.	Oxehealth has tooling which enables Clear Video Data to be remotely clipped and saved to a NAS at customer sites when requested by customers. Oxehealth technical staff are not able to view the data using this tooling. A small number of Oxehealth technical leads have access to the Egress account on which Clear Video data is stored where this data is provided to customers via Egress for Serious Incident review. Oxehealth access Anonymised (blurred) Video Data, Algorithm Processed Data, User Interface Output Data and System Performance Data on AWS UK servers remotely in order to support system configuration and maintenance activities, and/or restore data from a backup. This data is Pseudonymised and is not classed as personal data where Oxehealth do not have access to other data which would identify the individual Oxehealth staff with access to provide support for the Oxevision system use a unique set of credentials for VPN, remote machine access and file server access. VPN access requires 2 factor authentication, is audited and logging and pattern-based alerts are active on the VPN and firewall.

Data Privacy Impact Assessment

4	Will you be storing any NHS / LA data in hard copy for any length of time? <i>If so, how will the data be stored?</i>	No
5	Will you be storing any NHS/LA data in electronic format? <i>If 'Yes' complete 5a – 5h)</i>	As detailed in 1 above: 1. Data is stored on the local secure server at customer site as detailed in 1. Clear Video Data is automatically deleted by the software after 24hrs. All other data is deleted automatically after it has been uploaded to AWS storage. 2. Where Clear Video Data is provided to customers via Egress for Serious incident review this is recorded on Egress AWS or Azure servers in the UK for up to 30 days after which it is automatically deleted. 3. Anonymised (blurred) Video Data, Algorithm Processed Data, User Interface Output Data and System Performance Data is stored in Oxehealth's AWS UK secure storage. This data is Pseudonymised and is not classed as personal data where Oxehealth do not have access to other data which would identify the individual. 4. Occasionally if requested by customer staff to resolve a complex issue with the medical device Oxehealth will transfer Clear Video Data on a NAS and ingest it to Oxehealth secure servers at Oxehealth's UK site.
5a	Do all users of your systems have their own log-in and password?	Oxehealth staff are required to have individual logins for all Oxehealth systems and services which they access. Oxehealth staff with access to provide support for the Oxevision system use a unique set of credentials for VPN, remote machine access and file server access. VPN access requires 2 factor authentication, is audited and logging and pattern-based alerts are active on the VPN and firewall. Customer staff do not have access to stored data. They access a user interface on tablets

Data Privacy Impact Assessment

		which are pin protected or a fixed screen which is located in a secure location (such as a nurses station) in order to view and respond to real time movement alerts or take vital signs measurements.
5b	How are access rights to systems controlled?	Oxehealth has implemented OX.POL.029 Access Control Policy which establishes logical and physical access control rules, access rights and restrictions for specific user roles towards information and infrastructure assets appropriate to the level of risk. For any systems or services which contain or through which customer PII can be processed the assignment and maintenance of permissions and rights are restricted to trusted administrator and senior roles with procedures for authorisation, revocation and audit defined in the OX.PRO.054 PII and PHI Data Authorisation Process. Administrator and privileged access to infrastructure and services is reviewed as roles change and is audited at least annually. In addition the OX.POL.039 Network Access Control Policy defines the rules for connection of only approved devices to the Oxehealth Network.
5c	Are back-ups encrypted?	Backups are encrypted in transit and at rest to a minimum of AES-256 standard.
5d	What protection do you have against malicious code?	Oxehealth operates antivirus and malware protection software in its laptop, desktop and server builds wherever possible, and users are to ensure that no restrictions prevent antivirus and anti-malware software from operating as intended. In addition Oxehealth ensures code within the Oxevision software is safe through static analysis at the build phase, vulnerability scanning against industry standard vulnerability databases as part of pre-release testing, and external penetration testing by crest accredited penetration testers at least twice annually.
5e	How often do you apply security patches?	Security patches are applied to Oxehealth infrastructure on a weekly basis. Security patches are applied to Oxevision on customer sites in a rolling 6 week release cycle.

Data Privacy Impact Assessment

5f	How often do you risk assess your security controls?	Oxehealth participates in security feeds, carries out monthly vulnerability scanning of infrastructure and monitors risks as part of monthly security review meetings which are part of the OX.PRO.063 Information Security and Privacy Management Review Process. In addition risks and controls in the security risk register and/or new risks are reviewed as part of change management, in response to internal or external feedback and following an incident or potential incident, and a full review is also carried out at least once annually according to the OX.PRO.065 Information Security and Risk Management Process.
5g	What business continuity/disaster recovery plans do you have in place?	Oxehealth has established the OX.FWK.071 Oxehealth Business Continuity and Disaster Recovery Framework for assessing business continuity risk, identifying critical infrastructure and services, and implementing measures and plans which are continuously improved through ongoing monitoring and testing to ensure resilience and recovery capabilities. The framework incorporates the following Business Continuity Plans: • OX.PLN. 370 Oxehealth Facilities Business Continuity Plan • OX.PLN. 371 On-Premise Production System Business Continuity Plan - OX.PLN.369 Pandemic Business Continuity Plan • OX.PLN.214 Malicious Employee Business Continuity Plan
5h	Are USB ports/CD writers on staff equipment disabled?	USB ports on Oxehealth endpoints are not disabled, however Oxehealth's OX.POL.050 Storage and Protection of Information Policy prohibits staff from making or storing local copies of Customer PII on their local devices. Oxehealth have additionally established the OX.POL.046 Removable Media Policy which provides rules to Oxehealth employees for the use of removable media. This policy requires authorisation before customer PII it is copied from servers which store patient data to removable and state that the Oxehealth Data Protection Officer must be notified when this happens. It further requires all data to be encrypted before being placed onto removable media according to OX.POL.033 Cryptographic

Data Privacy Impact Assessment

		and Key Management Policy and only Oxehealth provided NAS's and encrypted USB's are to be used
5i	Will you be storing data outside the UK? <i>If so, where? What information governance considerations have been taken into account?</i>	No patient data generated by the Oxevision system will be stored outside the UK A small amount of customer staff information (name, job role, email address, telephone number) is stored in Google Drive (EU) for use by Oxehealth's customer success and operations teams to communicate and arrange meetings with customers for site installs, training, etc and (name, email address) is stored in Gitlab (USA) as part of the customer site configuration to configure the delivery of reports from the Oxevision system. Data processing addendums are in place with Google and Gitlab and security measures and safeguarding measures for data transfers have been assessed as appropriate to the level of risk to data subjects.
6	Will the data be linked with any other data collections? <i>If so, how will the link be achieved?</i>	No
7	What security controls do you have in place for your office premises?	Oxehealth has established OX.POL.069 Physical Security Plan which defines the physical perimeter of Oxehealth premises covered by Oxehealth's ISO 27001 and ISO 27701 certified Information Security and Privacy Management System, and lays out the policies and plans for controlling access and protecting the premises and equipment from external and environmental threats. Security controls in place include: • Physical locks on entry doors and doors to restricted areas. • A door access control system with per person restriction on access to Oxehealth premises and restricted areas, and logging of all door entries. • Internal locks on all openable windows • A system for signing in visitors • An intruder alarm system and 24/7 security services • CCTV in locations that cover main entry points, main office, foyer, entry to restricted areas and inside restricted areas

Data Privacy Impact Assessment

8	What controls do you have in place for the security of your equipment?	Physical security in place as described in 7 above including limited per person access and logging for restricted areas (including Oxehealth's server room) In addition Oxehealth has a workstation use policy which covers the use of equipment by Oxehealth staff on the Oxehealth premises and outside the premises. Technical measures include • individual domain login with secure passwords which follow Oxehealth's OX.POL.040 Password and Multifactor Authentication Policy. • Remote access via VPN with 2 factor authentication for remote / hybrid workers • Encryption using BitLocker or Lucks • Rules in place to prevent installation of unauthorised software according to the OX.POL.051 Unauthorised Software, Malware and Anti-Virus Policy. • Installation of end-point detection and recovery software • Segregation of duties with most users not permitted to have admin rights and authorisation and separate accounts required for users with admin rights according to the OX.POL.049 Segregation of Duties Policy.
9	Have you had any security incidents relating to data in the last three years? <i>If so, please provide details.</i>	No
10	What policies do you have in relation to information security, data protection and incident reporting? <i>Please provide copies.</i>	Oxehealth has established an information security and privacy management system is externally audited and certified to ISO 27001 and ISO 27701 standards. There OX.POL.004 Oxehealth Information Security and Privacy Policy is the top level policy in the management system which establishes Oxehealth's overall commitment to security and privacy and is supported by many other policies and procedures. As part of the Oxehealth ISMS and PIMS Oxehealth have also established a number of procedures including the OX.PRO.062 Security

Data Privacy Impact Assessment

		and Privacy Incident Management Process to ensure a consistent and effective approach to the management of information security incidents, including incident reporting.
11	Describe potential disciplinary actions for breach of policy.	Oxehealth has implemented OX.POL.047 Sanctions Policy to • define and ensure employees are aware of their responsibilities for upholding the policies and procedures in the ISMS and PIMS and for complying with applicable data protection regulations and the consequences if they fail to uphold these responsibilities. • Provide guidance for management on the appropriate level of disciplinary procedures to apply should employees fail to comply with the ISMS/PIMS policies and procedures and applicable regulations. The level of disciplinary action is dependent on the nature and severity of the indiscretion and may include formal warnings or dismissal.
12	How do you ensure the people your recruit have the honesty and integrity to handle personal data?	Oxehealth has implemented OX.POL.041 Personnel Security and Privacy Management Policy which sets out the ways in which Oxehealth ensures its employees are trained and onboarded, and the checks and balances Oxehealth puts in place to mitigate the risks to Oxehealth of employee negligence or 'bad actors' and any knock-on impact to our customers and their patients. The policy requires background checks to be carried out on all new employees which include third party reference checks (at least 2) before starting employment and security checks (BPSS, DBS or similar) dependent on role and country during the onboarding process.
13	How do you ensure your staff understand the importance of data security and how to keep personal data secure?	The OX.POL.041 Personnel Security and Privacy Management Procedure requires all employees to be trained on essential information security and privacy information, and quality policies and processes including as part of their onboarding including followed by annual refresher training thereafter. Additional security and quality training is required for specific roles and is determined by

Data Privacy Impact Assessment

		the line manager, along with the security and quality managers according to the OX.PRO.022 Staff Competence and Training Process
14	How frequently do you provide your staff with training on data security / confidentiality and is their learning tested?	Training is carried out at least once every twelve months or sooner following changes to policies or changes to staff roles. All training is tested with a minimum pass rate of 80%
15	Will you ever transfer NHS/LA data electronically? <i>If so, how?</i>	Yes – data generated by the Oxevision system is transferred as follows: • Uploaded via secure SSL AES256 encrypted connection to amazon web servers. • Activity tracker and vital signs trends are emailed to clinical staff in the form of reports- these do not contain any patient identifiable information. • Single frame images of empty rooms are transferred to Oxehealth secure servers as part of system configuration and when required to address any issues with the system. Oxehealth uses tooling to ensure there are no people in the images. • Where Clear Video data is provided to customer staff for serious incident review this is either copied to an encrypted password protected USB device and handed to customer staff by a field agent attending customer site, or it is delivered via Egress Secure Workspace where it is encrypted to AES 256 standard in transit and at rest. • Where Oxehealth is instructed to review Clear Video data to resolve a complex issue with the medical device this is encrypted and copied to a NAS and transported to Oxehealth where it is ingested into Oxehealth's local secure servers at their UK office.
16	Will you transport any NHS/LA hard copy data? <i>If so, what security controls will be in place?</i>	No
17	Will you ever destroy any NHS/LA data? <i>If so, what method is used and what evidence of destruction will be provided?</i>	All data generated by the system is automatically deleted by the software or within storage according to set retention policies. Any data stored on local secure servers at customer sites at the end of the customer contract will be destroyed as part of site

Data Privacy Impact Assessment

		decommissioning as per the service agreement signed with customers. Oxehealth has implemented a process which includes securely scrubbing (deleting) the data from all electronic storage media. The hard drives are then removed and disposed of using a secure method such as shredding or degaussing. The hard drive disposal will be through a certified third party and Oxehealth will require certificates of destruction for these.
18	Will you ever sub-contract work in relation to NHS/LA data? <i>If so, in what circumstances?</i>	First line support for the Oxevision system is sub-contracted to 3C Online. This means that 3C online will process support calls and emails sent by Oxehealth customers. Oxehealth warns customers not to include any patient personal information in emails or over the telephone but there is a risk a small amount of data will be shared. Oxehealth has signed a data processing agreement with 3C Online and they are required to use the Oxehealth provided ticketing system for support. The system has tooling available which enables Oxehealth to redact any patient personal data accidentally shared by customers.
Date completed:		29 November 2023
Completed by:		Tammarin Coffin, Data Protection Officer
Telephone number and email address:		Privacy@Oxehealth.com  DPIA - Oxevision Only UK v29 (1).docx

Appendix 2 – Glossary of Terms

Item	Definition
Personal Data	This means data which relates to a living individual (data subject) who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person: A) from those data, or B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Special Categories of Data	This means personal data consisting of information as to the: A) racial or ethnic origin of the individual B) the political opinions of the individual C) the religious or philosophical beliefs of the individual D) whether the individual is a member of a trade union E) processing of genetic or biometric data for uniquely identifying an individual F) physical or mental health of the individual G) sex life or sexual orientation of the individual
Direct Marketing	This is “junk mail” which is directed to particular individuals. The mail which are addressed to “the occupier” is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.
Automated Decision Making	Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means including profiling, which produces

	legal effects concerning the data subject or similarly affects them. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned.
International organisation	Means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
Explicit Consent	Express or explicit consent is given by the data subject freely given, specific, informed and unambiguous indication of the data subjects wishes, usually orally (which must be documented in the patients casenotes) or in writing, to a particular use of disclosure of information.
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population

	may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to

	keep records longer than 30 years must obtain approval from The National Archives.
Information Governance Alliance (IGA) Records Management NHS Code of Practice	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
General Data Protection Regulation (EU) 2016/679 (GDPR)	European legislation (applied in UK law by the Data Protection Act 2018) on the protection of natural persons with regard to the processing of personal data. The Regulation defines the ways in which information about living people may be legally used and handled. The 6 principles of the Regulation state the fundamental principles relating to processing personal data must: • be processed fairly and lawfully. • Collected for specified, explicit and legitimate purposes • be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • be accurate and, where necessary, kept up to date. • Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. • be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. The Regulation also requires that the Data Controller and Data Processor are both able to demonstrate compliance with these principles.
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.
Article 6 Conditions of Processing	1) (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes - only lawful if ALL article 7 conditions for consent are met 1) (b) A contract with the individual: for example, to supply goods or services they have requested, or to fulfil your

	obligations under an employment contract. This also includes steps taken at their request before entering into a contract. 1) (c) Compliance with a legal obligation: if you are required by UK or EU law to process the data for a particular purpose, you can. 1) (d) Vital interests: you can process personal data if it's necessary to protect someone's life. This could be the life of the data subject or someone else. 1) (e) A public task: if you need to process personal data to carry out your official functions or a task in the public interest – and you have a legal basis for the processing under UK law – you can. If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities. 1) (f) Legitimate Interest: If you need to process personal data in the legitimate interests of the Data Controller or 3rd Party or Data Subjects Rights in particular where data subject is a child. NB 1) (f) does not apply to processing carried out by Public authorities in the performance of their tasks.
Article 9 Conditions of Processing special categories of data	(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (2) Paragraph 1 shall not apply if one of the following applies: 2) (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject only lawful if ALL article 7 conditions for consent are met (see column D)" 2) (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

- 2) (c) 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;
- 2) (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- 2) (e) processing relates to personal data which are manifestly made public by the data subject;
- 2) (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- 2) (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- 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;
- 2) (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- 2) (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to

	safeguard the fundamental rights and the interests of the data subject.
Article 7 (Recital 32) Conditions for Consent	Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Appendix 3 – Examples of Risk

EXAMPLES OF PRIVACY AND RELATED RISKS	
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 peoples 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 that individuals may 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 of the disclosure of information.	
Collecting information and linking identifiers may 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 is necessary.	
CORPORATE RISKS	
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 fines.	
The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engagement 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 organisations reputation and lead to loss of business.	

Data Privacy Impact Assessment

Data losses which damage individuals could lead to claims for compensation.

COMPLIANCE RISKS

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