

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 [[HYPERLINK "mailto:tewv.dpia@nhs.net"](mailto:tewv.dpia@nhs.net)]

Further guidance on DPIA can also be found on the Information Commissioner's website [[HYPERLINK "http://www.ico.gov.uk"](http://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	Oxehealth Sleep Module Pilot
DPIA number:	DPIA 730 (see also DPIA 065)
Project Description	
Name and Job title:	Alison McIntyre, Associate Director of Nursing/SRO for Oxehealth Project [i/s] Senior Project Manager
Date:	04/02.2024

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.

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.

There is currently an approved DPIA for the use Oxehealth in the trust. This DPIA 065 [[HYPERLINK "file:///T:/Data%20Protection%20Impact%20Assessment/DPIA%20LIBRARY/05.%20051%20-%20100/CSI065%20Oxehealth%20Monitoring%20System/CSI065%20Oxehealth%20VBPM%20v1.0%20Approved.docx"](file:///T:/Data%20Protection%20Impact%20Assessment/DPIA%20LIBRARY/05.%20051%20-%20100/CSI065%20Oxehealth%20Monitoring%20System/CSI065%20Oxehealth%20VBPM%20v1.0%20Approved.docx)] is underpinned with policy and written procedures and should be considered alongside this activity.

Sleep Module

This DPIA covers the use of piloting a sleep module within the Oxehealth tool with the trust acting as an early adopter. This is a new medical device that will form part of the Oxehealth platform.

Sleep Monitoring gives clinicians access to objective data on a patients sleep pattern by analysing vital signs and activity data from Oxehealth's infrared-sensitive camera giving them more insight to support patient-centred clinical decision-making as well as improve the overall ward sleep environment. No new categories of data are introduced; existing categories are updated to include sleep data.

Data Privacy Impact Assessment

Daily outputs are readily available in a graphical timeline showing when the patient was in bed and asleep versus in bed and awake, and as summary sleep metrics (e.g. total sleep time). It should be noted that to obtain sleep data the image recorded on Oxehealth is not accessed but the unit needs to be on.

The following wards have had the software installed but it is not yet live: Cedar, elm, rowan-lea, westerdale-south, wold-view, Lustrum vale, Stockdale and Bilsdale.

The pilot will take place with cedar ward and elm wards west park hospital and Rowan Lea, cross Lane Hospital Scarborough. This will start once the DPIA and Clinical Safety Case have been approved and training with ~~teh~~ the wards has taken place – likely to be March 2025. Other wards and dates are to be confirmed.

The policy and procedures will be considered when looking at its implementation

If the pilot is successful and when it moves to business as usual the Oxehealth DPIA (065) will be updated and reviewed.

The Privacy Notice will be considered [HYPERLINK
"https://www.tewv.nhs.uk/about/publications/privacy-notice/" \h]

The Clinical Safety Case is also being considered

Due diligence and a technical security check have previously been undertaken but that if the pilot is successful when the DPIA 065 is reviewed the updated 3rd Party assessment will be refreshed.

Questions	Yes	No
Will you collect new information about individuals or compel them to provide information about themselves?	☒	☐
Will information be shared to organisations or people who have not previously had access to the information? (including processing by 3 rd parties)	☒	☐
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?	☒	☐
Will you use systematic and extensive profiling or automated decision making to make significant decisions about people?	☐	☒
Will you process special category data (sensitive data) or criminal offence data on a large scale? (<i>Sensitive includes health information</i>)	☐	☒
Will you systematically monitor a publicly accessible place on a large Scale?	☐	☒
Will you be using any new technologies or technologies which might be perceived to be privacy intrusive e.g. processing biometric or genetic data?	☒	☐

Data Privacy Impact Assessment Proforma Ref: [DPIA 730](#)

pg 3

TEWV DPIA Template v1.6 July 2024

[FILENAME * MERGEFORMAT]

Data Privacy Impact Assessment

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?	☐	☒
Will you carry out profiling on a large scale?	☐	☒
Will you combine, compare or match data from multiple sources?	☐	☒
Will you process personal data without providing a privacy notice directly to the individual?	☐	☒
Will you process personal data in a way which involves tracking individuals' online or offline location or behaviour?	☒	☐
Will you process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them?	☐	☒
Will you process personal data which could result in a risk of physical harm in the event of a security breach?	☐	☒

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 **[HYPERLINK "mailto: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 **[HYPERLINK "mailto:tewv.dpia@nhs.net"]**

Section B - Full Data Protection Impact Assessment (DPIA)

Form completed by:

Name:	Alison McIntyre/[I/S]
Job Title:	Associate Director of Nursing/SRO for Oxehealth Project/ Senior Project Manager
Signature:	
Date:	4.02.2025

Name of System / Project:	Oxehealth – Sleep Module
Data Controller details:	TEWV
Data Processor details:	Oxehealth
Objective:	Expanding the use of Oxehealth to monitor sleep to improve patient safety and care
Background: Why is the new system / change in system required?	Oxehealth, is a Vision Based Patient Monitoring System, an assistive tool that enhances and supports patient safety within inpatient services has been used successfully over the past 5 years with no recorded information incidents. We are now looking to expand the use of the system to include sleep monitoring module and are participating in an early adopter initiative to pilot in several agreed wards. This will enable us to monitor sleep patterns to inform clinical practice and development of individualised care planning. Whilst the Oxehealth system is required to generate the report, images are not accessed at any point. The report is produced in PDF by room number only and the data does not contain any patient identifiable information. Oxehealth sleep module will use a consent-based model allowing patients to opt-out after 72 hours of admission.

Data Privacy Impact Assessment

Benefits:	Sleep Monitoring gives clinicians access to objective data on patient sleep patterns by analysing vital signs and activity data from Oxehealth's infrared-sensitive camera, although no image is viewed. This will enable MDTs to monitor sleep patterns to inform clinical practice and development of individualised care planning and promote sleep hygiene. Sleep hygiene supports in mental health recovery and can reduce patient safety related incidents. Daily outputs are readily available in a graphical timeline showing when the patient was in bed and asleep versus in bed and awake, and as summary sleep metrics (e.g. total sleep time). This is a PDF version by room number only with no identifiable patient related information.	
Constraints:	Hardware and server administration is provided and managed by third party. Trust infrastructure for Wi-Fi 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:	This is a medical device that provides accurate data which will allow monitoring of sleep patterns to inform clinical practice, improve patients' outcomes and reduce sleep related incidents.	
Cross reference to other projects:	Oxehealth DPIA 065 [HYPERLINK "file:///T:/Data%20Protection%20Impact%20Assessment/DPIA%20LIBRARY/05.%20051%20-%20100/CSI065%20Oxehealth%20Monitoring%20System/CSI065%20Oxehealth%20VBPMs%20v1.0%20Approved.docx" \h]	
Project Manager:	Name:	[I/S] /Alison McIntyre
	Title:	Senior Project Manager /ADON
	Department:	Assistant Chief Executive's /SIS - DTVF
	Telephone:	07341097350
	Email	[HYPERLINK "mailto:[I/S]" \h] [HYPERLINK "mailto:[I/S]" \h]

Data Privacy Impact Assessment

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:	07970 692408
	Email	[HYPERLINK "mailto:[I/S] \h]

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)	Name:	[I/S]
	Title:	End User computer Manager
	Department:	Digital and data Services
	Telephone:	07918330143
	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)	SRO – Alison McIntyre, Chief Nurse, Deputy Chief Nurse, TEWV Oxehealth Steering Group, TEWV Oxehealth Clinical Subgroup, TEWV Oxehealth installation group, Oxehealth Co Creation Subgroup, Patients, Carers/Families. Project management framework – Oxehealth Steering feeding into Patient Safety Programme Board, feeding into Transformation and Strategy Board.	

Section C - Privacy Impact Assessment Key Questions

Question	Response	Ref to key req. e.g. GDPR, DPA18 etc
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 If yes, please specify: ☐ Patient ☐ Staff ☐ Other (specify) Click or tap here to enter text.	

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 monitoring sleep will be adopted. Oxehealth isn't envisaged to take the place of staff therefore BAU as per the SOPs will be in place	2	1	2
Service users not being appropriately informed of the Trust's processing activity and collection of sleep module data.	4	3	12	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	4	2	8

Data Privacy Impact Assessment

				across the Trust and will contribute to achieving the mitigation of this risk. Policy and procedure approved and has been rolled out to all wards with Oxehealth currently and will be rolled out as each new ward goes live with oxehealth. This will involve staff visiting the wards and undertaking training with ward staff. Monthly audit re: use of Oxehealth and model of consent.			
The sleep data will not be available if the patient has chosen to opt out of oxehealth	3	3	9	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 decision recommending that the VBPMS be switched off or on for the individual patient., based upon	2	3	6

Data Privacy Impact Assessment

				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 there will be a number of trigger events will initiate further reviews of the required status of the VBPMS (i.e., whether it is “switched on” or “switched off”). If patients do opt out of the system and sleep is required to be monitored, normal process/procedures can be adopted.			

Data Privacy Impact Assessment

Data Privacy Impact Assessment Proforma Ref: [DPIA 730](#)

[TEWV DPIA Template v1.6 July 2024](#)

[FILENAME * MERGEFORMAT]

pg 12

Section E - Sign off, actions and outcomes

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

DPIA Reviewed by	[I/S] Information Compliance Manager	Review Date	12/02/25
IT Servicedesk Reference:	n/a	DPIA Central Register Reference	730
Summary of IG Advice: Support offered with the completion. Clarification sought that to access the sleep data the unit needs to be on the clinician doesn't need to access the images therefore a full DPIA is not required. With this in mind a risk has been added to reflect the fact that policy allows patients to opt-out of having the unit on. To go to IGG 19/02/25			
Action Assigned	Responsibility	Due	Completed
Click here to enter text.	Click here to enter text.	asap	Click here to enter text.
Risk Mitigations approved by: (a person of seniority on the project)	Click here to enter text.		Click here to enter text.
Remaining Risks accepted by: (a person of seniority on the project)	Click here to enter text.		Click here to enter text.
Can the DPIA be passed to Data Protection Officer for Approval?	☐ Yes FORMCHECKBOX No Click or tap here to enter text.		Click here to enter text.

Data Privacy Impact Assessment

DPO Advice Provided		☐ Yes ☐ No	Date
Summary of DPO advice:			
DPO advice accepted		☐ YES ☐ NO	<i>NB: If no state reason why below</i>
Comments:			
Residual High risk		☐ YES ☐ NO	<i>(if yes report to ICO)</i>
ICO Outcome:			
DPIA Approved		☒ YES ☐ NO	
DATE: <u>Approved at IGG on 19/02/25</u>			
<u>Approved at IGG on 17/04/25</u>			
<u>Approved at IGG on 17/09/2025</u>			
If no please justify			
Click or tap here to enter text.			
DPIA Review Due Date	<u>19/07/2027</u>	DPIA Owner	<u>Maxine Lawson</u>

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

Appendix 1 – Checklist for Third Parties

Tees, Esk and Wear Valleys NHS Foundation Trust (the Trust) and your organisation are currently in discussions regarding the provision of services by you to the Trust, which would involve your processing personal data on our behalf and/or the supply of IT systems, software or hardware.

The Data Protection Act 2018, UKGDPR Data Security and Protection Requirements imposes on the Trust certain requirements in relation to the selection and use of its data processors and suppliers of IT systems. We must, therefore, ask you – as a potential market supplier and or data processor to provide certain information to us so that we can determine whether you can provide sufficient guarantees in relation to the processing and an appropriate level of security for the data within the technologies to be used.

In the first instance would you please complete and return this questionnaire, signed by an authorised representative for your organisation.

Section A – Supplier / Processor Details

Your details	
Company Name	Oxehealth Limited, Registered in England and Wales, Company Registration Number 08163325
ICO Reg No.	ZA065748
Address	Magdalen Centre North, The Oxford Science Park, Littlemore, North OX4 4GA
Contact name	Tammarin Coffin/[I/S]
Contact details	Telephone: :
	Fax:
	Email:[I/S]

Section B – Accreditations

Please indicate which security accreditation / certification you currently hold by ticking the appropriate option and embedding a copy of the certificate:

Standard	Description	Yes	No	N/A
ISO/IEC 27001	A current ISO/IEC27001:Information Security Management certificate issued by a United Kingdom Accreditation Service (UKAS)-accredited certifying body and scoped to include all core activities required to support delivery of services to the customer. Certificate Number: 172589  Oxehealth ISO 27001 certificate exp	☒	☐	☐
Cyber Essentials (CE) certification	A current CE certificate from an accredited CE certification body Certificate Number: aa1c77bf-a477-4f6f-8875-a8cfd696951c  Oxehealth Cyber Essentials Certificate	☒	☐	☐
Cyber Essentials Plus (CE+) certification	A current CE+ certificate from an accredited CE+ Certification Body. Certificate Number: 4bf4d0ce-9572-4d87-bd91-62411ade8661	☒	☐	☐

Data Privacy Impact Assessment

	 Oxehealth Cyber Essentials Plus Certi			
NHS Data Security and Protection Toolkit (DSPT)	The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. To provide assurance that they are practising good data security and that personal information is handled correctly. ODS Code: 8K867 Latest Status and date published: Standards Exceeded 27 June 2024  2023-24 (version 6) 8K867 DSPT standard	☒	☐	☐
Other types of certification	Please provide evidence of anything which you think is relevant and would like us to consider ISO/IEC 27701 Certificate Number: 188309  Oxehealth ISO 27701 certificate exp	☒	☐	☐
No accreditation / certification	The Organisation does not have any of the above accreditations	☐	☒	☐

Section C– Security Policies & Procedures

Your security policies and procedures	Yes	No	N/A
Do you have an information security policy? If yes, please provide a copy	☒	☐	☐

Data Privacy Impact Assessment

Your security policies and procedures		Yes	No	N/A
 OMS-OX.POL.004 Oxehealth Informati  OMS-OX.DOC.091 Oxehealth Informati OX.POL.004 Oxehealth Information Security and Privacy Policy is attached along with OX.DOC.091 Oxehealth Information Security and Privacy Manual. The security policy is a top level policy, the manual lists all the policies and procedures in the ISMS. The top level policy does not include all the information in the below list, but this is included in other topic specific policies or in other ISMS documents.				
Does your information security policy include the following: (Note: The following are included in topic specific policies which are part of the overarching security policy, and not in the security policy itself)				
• Physical security of premises and processing areas		☒	☐	☐
• Physical entry controls		☒	☐	☐
• Equipment security and maintenance (Inc. physical device security)		☒	☐	☐
• Password and access controls		☒	☐	☐
• Encryption of personal data on all mobile devices		☒	☐	☐
• Encryption of personal data on desktop computers and devices		☒	☐	☐
• Encryption of personal data on storage devices and backup		☒	☐	☐
• Controls against malicious software		☒	☐	☐
• Controls against denial of service attacks		☒	☐	☐
• Controls against hacking		☒	☐	☐
• Business continuity planning		☒	☐	☐
• Monitoring system access and use (including audit trails)		☒	☐	☐
Do you have a policy for complying with the Data Protection Act 2018 (incorporating the General Data Protection Regulation (GDPR)? If yes, please provide a copy OX.POL.097 Personal Data Collection and Processing Policy  OMS-OX.POL.097 Personal Data Collec		☒	☐	☐

Data Privacy Impact Assessment

Your security policies and procedures		Yes	No	N/A
Do you have a data breach policy? Data breaches are covered in our Incident Management Policy (attached above) and also in our Incident Management Policy (attached below) If yes, please provide a copy OX.POL.062 Security and Privacy Incident Management Policy  OMS-OX.PRO.062 Security and Privacy		☒	☐	☐
Do you have a clear desk policy or is covered in another policy?		☒	☐	☐
Do you have a clear screen policy or is it covered in another policy?		☒	☐	☐
Do you have a secure disposal policy for equipment, media and data?		☒	☐	☐
Do you disable USB ports/CD writers on staff equipment? Ports are disabled for most staff equipment with exceptions for some roles.		☒	☐	☐
Please describe how you risk assess your security controls including the frequency? We conduct regular risk assessments of our security controls as part of our ISO 27001 certified Information Security Management System (ISMS). Risk assessments are performed at least annually and additionally triggered by key processes such as incident management, corrective and preventive actions (CAPA), vulnerability management, security management review, and our secure software development lifecycle. Security controls are reviewed and updated based on identified risks, regulatory changes, and emerging threats.				
Please describe how you dispose of paper records and electronic records: We follow OX.POL.036 Media Re-Use and Disposal Policy and Procedures for the disposal of both paper and electronic records. Staff are required to use a cross-cut or micro-cut shredder for paper records containing sensitive or confidential information. Note, staff are not permitted to print any information generated by the Oxelevision system. Electronic records are securely deleted in accordance with their retention policies using appropriate secure deletion techniques such as data shredding or other industry standard methods.				

Data Privacy Impact Assessment

Your security policies and procedures		Yes	No	N/A
Please describe the measures you have in place to prevent unauthorised access to your systems from outside your company: Oxehealth has multiple security measures in place to prevent unauthorised access to our systems. These include firewalls, remote access via VPN, role based access controls with multi-factor authentication (MFA) and encryption of data at rest and in transit. We enforce mobile device management (MDM) and industry-standard endpoint protection and recovery on user devices. Our cloud hosted infrastructure is secured using industry-standard encryption protocols, and we actively monitor system activity for suspicious behaviour. Unauthorised access attempts are logged and investigated as part of our incident response. We run industry standard vulnerability scanning tools across internal infrastructure and production systems, mitigating vulnerabilities according to severity. Oxehealth's internal infrastructure undergoes annual external testing as part of Cyber Essentials Plus while our production systems are tested by crest-accredited penetration testers. Staff receive regular security awareness training and are required to comply with all security policies and procedures.				
Do you have a backup and disaster recovery policy? The OX.FWK.071 Oxehealth Business Continuity and Disaster Recovery Framework includes Oxehealth's policy for resilience planning, data backup, failures, disasters and disaster recovery modelling and business continuity planning. This document is not externally shareable as it contains some security secrets. The production system business continuity plan for Oxevision is attached below. If yes, please provide a copy  OX.PLN.371 On-Premise Product		☒	☐	☐
Please indicate what virus detection and prevention software you use: Sentinel One is used on internal infrastructure. Production systems are scanned against the NIST NVD vulnerability database and are subject to twice annual penetration tests.				
How often do you apply security patches to your systems? We apply security patches based on a risk-based approach, prioritizing vulnerabilities by severity and impact. For internal infrastructure, critical vulnerabilities that could affect our environment are patched within 24 hours, while others follow a 72-hour to two-week timeline. High-risk issues are patched within a month. Additionally, security updates for staff endpoints, such as Windows patches, are automatically applied a week after release. For our Oxevision production system, critical vulnerabilities are patched urgently via hotfixes or the next available release. High-risk patches are included in the next release, while medium-risk patches are scheduled based on risk assessment. This ensures timely remediation while minimizing disruption				
Please confirm where the data resides?				

Data Privacy Impact Assessment

Your security policies and procedures	Yes	No	N/A
Data generated by the Oxevision system is stored on local servers at customer sites. Anonymised video, algorithm data, user interface output data and logs are then backed up to AWS. (UK residency).			
Do you have any equipment off-site or store any personal data off-site? If so, please describe the measures you have in place to prevent unauthorised access to that equipment or storage facility As mentioned above some anonymised data is backed up to AWS. This data is encrypted in transit to at least TLS 1.3 and encrypted at rest to AES-256 standard. Strict access controls which include at least two factors of authentication are implemented to ensure only authorised staff have access, and automated monitoring has been implemented with alerts to any unusual activity. Oxehealth regularly monitors the security posture of AWS through review of their SOC reports and security certifications.	☐	☒	☐
Do you or will you as part of the service you will provide to the Trust, transfer or process any of the Trusts personal data outside of the United Kingdom? If yes, please provide details of what you will transfer, how this will be transferred and to which country: No patient data generated by Oxevision will be stored outside of the United Kingdom However some customer staff email addresses for receiving reports are stored in configuration files in Gitlab and the data is stored in the US. Gitlab have signed a data processing addendum with Oxehealth which includes SCCs and an IDTA has been carried out.	☒	☐	☐
Will the data you will use or process for the Trust be linked to any other data collections? If yes, how will the link be achieved?	☐	☒	☐
Do you confirm you will only be using and retaining data as per the detail in the agreed contract / DPIA? <i>(please note this may still be being negotiated)</i>	☒	☐	☐
Do you have a written procedure for storage of customer records? We do not have a shareable internal procedure, however information on all data generated by the system, the data flows, storage and retention are included in the Oxevision DPIA and Data and Governance Overview. If yes, please provide a copy  Oxevision DPIA and Data and Governance	☐	☒	☐

Section D– Cloud security and governance

If you are using any cloud storage as part of this activity please answer the following questions.
If not please advance to section E

Cloud Security and Governance	Yes	No	N/A
Is communication of Personal Identifiable Information (PII) to and from the cloud storage always encrypted to a TLS 1.2 / AES 256 or higher (Encryption in Transit)?	☒	☐	☐
Is PID stored in the cloud always encrypted to a TLS 1.2 / AES 256 or higher (Encryption at rest)?	☒	☐	☐
Are other customers of the cloud service provider using the same storage servers?	☐	☒	☐
Are there robust systems in place to prevent unauthorised access or unintended/accidental leakage between different customer environments in the cloud storage? Each customer has segregated storage which is controlled by customer specific key/certificate authorisation. Customer A has no access to Customer B's certificate pair.	☒	☐	☐
Cloud Security and Governance	Yes	No	N/A
Can the data in the cloud server be made inaccessible to the cloud server provider? E.g. by encryption controlled by the application provider? This should include both patient and user data. All data is encrypted and the cloud server provider does not have access to decryption keys	☒	☐	☐
Is high availability assured during UK working hours? Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. There would be no impact on the system if the cloud data was unavailable as the purpose of this data is for backup and post-market surveillance.	☒	☐	☐
In the event of cloud service termination of contract is there an agreement and demonstration of systems to ensure that data will be transferred to another acceptable location? The agreement states AWS will allow customers to retrieve content from services after termination. Oxehealth will use AWS tooling to securely transfer the data to another storage location.	☒	☐	☐

Data Privacy Impact Assessment Proforma Ref: [DPIA 730](#)

pg 22

TEWV DPIA Template v1.6 July 2024

[FILENAME * MERGEFORMAT]

Data Privacy Impact Assessment

In the event of cloud service termination of contract is there an agreement and demonstration of systems to ensure that following successful transfer of data that the data will not persist in the original cloud storage? Ensuring the data is transferred and deleted is Oxehealths' responsibility. Oxehealth will use AWS tooling to securely delete the data following transfer. The data will remain encrypted at all times and AWS do not have access to decryption keys.	☐	☒	☐
How quickly will the cloud provider react if a security vulnerability is identified in their product? AWS aims to react very quickly to identified security vulnerabilities, typically providing a patch or fix within a short timeframe, often within hours or days of discover, and will actively inform customers about the issue and mitigation steps promptly.	☐	☐	☒
How quickly could the cloud provider restore the data from a back-up if it suffered a major data loss? S3 storage is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. AWS stores data redundantly across multiple devices within a single Availability Zone			

Section E– Application security and governance

Your application security and governance	Yes	No	N/A
If appropriate what data item will you use as a primary identifier? If the trust implements user auth, this would be the subject value provided back from your Identity Provider.	☒	☐	☐
Can user access be restricted to only that required by each individual or organisation? Yes with User Auth enabled – Role based access control can be enabled at the trust's request.	☒	☐	☐
Is 2-factor authentication available? As we use OIDC when user auth is enabled, the login process is completed using the organisations Identity Provider	☒	☐	☐
Can the data user switch to anonymous display of data? (e.g. when viewing or sharing patient data where others might see) On sites where Oxevision Observations is not in use, the user interface does not display patient names or other identifiers such as NHS numbers, it displays room and ward names. Only the take vitals workflow which requires viewing up to 15 seconds of clear video data displays personal data. This functionality can be placed behind user auth if the trust requests it, meaning an unauthorised user is unable to view this data. As it is not possible to use the take vitals workflow without displaying clear video we would recommend not viewing this where others might see.	☐	☒	☐

Data Privacy Impact Assessment Proforma Ref: [DPIA 730](#)

pg 23

TEWV DPIA Template v1.6 July 2024

[FILENAME * MERGEFORMAT]

Data Privacy Impact Assessment

Section F– Employees

Your employees	Yes	No	N/A
Do you carry out verification checks on all potential employees?	☒	☐	☐
Do you have a personnel screening and vetting policy? If yes, please provide a copy See OX.POL.041 Personnel Security and Privacy Management Policy  OMS-OX.POL.041 Personnel Security a	☒	☐	☐
Do you ensure the reliability of employees who process personal data through an approved process? If yes, please provide details: We ensure the reliability of employees who process personal data through an approved process. This includes pre-employment screening, confidentiality agreements, regular data protection training, and strict access controls. Employees handling personal data are trained on GDPR compliance and information security, and access is granted based on role-based permissions	☒	☐	☐
Do you train staff on the care and handling of personal data and information security? If yes, please describe what this training involves and the frequency - All new starters receive onboarding training on their first week which includes training on GDPR, Security Awareness, Customer Data Handling (if relevant) and training on all other relevant security and privacy policies and procedures. - All staff receive annual refresher training on GDPR, Security awareness and relevant policies and processes. - Staff receive training on relevant policies and processes when changes are made to them as part of change management.	☒	☐	☐
Do your contracts with your employees include:			
confidentiality clauses?	☒	☐	☐
obligations to comply with information security and data protection policies?	☒	☐	☐
4- Potential disciplinary actions for breach of policy?	☒	☐	☐

Formatted: Indent: Left: 0.51", Hanging: 0.3", Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Section G– Contractors (Sub Processors)

Your contractors* (* this means any third party you appoint to process personal data on your behalf)	Yes	No	N/A
Will you use sub-processors to assist with the processing services for the Trust?	☒	☐	☐

Data Privacy Impact Assessment Proforma Ref: [DPIA 730](#)

pg 24

TEWV DPIA Template v1.6 July 2024

[FILENAME * MERGEFORMAT]

Data Privacy Impact Assessment

Your contractors* (* this means any third party you appoint to process personal data on your behalf)	Yes	No	N/A
If yes, please provide details of the contractual arrangements you have in place with them and confirmation that they are to the same level as any contract you will have in place with the Trust: Oxehealth signs data processing agreements with sub-processors which contain data protection obligations that are at least as restrictive as the obligations in our agreements with customers. A list of sub-processors is attached below:  Oxehealth Sub-Processors.pdf			
Have you taken steps to ensure that any sub-processors you will use to assist you with the processing services for the Trust have appropriate security measures in place for the personal data? Yes, we follow our OX.PRO.018 Supplier and Contractor Evaluation, Approval and Monitoring Procedure to assess the risk of all suppliers including sub-processors and agree measures and controls which are required. Evaluation of security measures include reviewing SOC reports, security certificates and policies and procedures.	☒	☐	☐
If yes, are you satisfied that the personal data will be adequately protected if you use these sub-processors?	☒	☐	☐
Do the contracts you have with your sub-processors impose obligations upon them to observe confidentiality and security in relation to any personal data which they may be required to process?	☒	☐	☐

Section H– Assurance

Your assurance	Yes	No	N/A
Have you been the subject of any complaints to the Information Commissioner (ICO) in the last 24 months? If yes, please provide details	☐	☒	☐
Have you ever had a security breach resulting in loss or unauthorised disclosure of personal data in the last 24 months? If yes, please provide details	☐	☒	☐
If deemed appropriate do you give approval for the Trust (or a trusted partner) to undertake on site security audit of your controls?	☒	☐	☐

Section I– Document Approval

Data Privacy Impact Assessment Proforma Ref: [DPIA 730](#)

pg 25

TEWV DPIA Template v1.6 July 2024

[FILENAME * MERGEFORMAT]

Data Privacy Impact Assessment

Please sign and date this questionnaire and return to your Tees, Esk and Wear Valley NHS Foundation Trust contact.	
Signed for and on behalf of Oxehealth Limited	
Print name	Tammarin Coffin
Position	Head of Data Privacy, Infosec & Contracts
Date	11 March 2025

[A](#)

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.

Data Privacy Impact Assessment

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

Data Privacy Impact Assessment

	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:

Data Privacy Impact Assessment

	• 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

Data Privacy Impact Assessment

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.

Data Privacy Impact Assessment

Public distrust about how information is used can damage an organisations reputation and lead to loss of business.
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