

Freedom of Information Request

Reference Number: EPUT.FOI.24.3458 (002)
Date Received: 1st May 2024

Information Requested:

1) I requested the approximate dates any documents were last reviewed and last updated. Please provide this information.

The documents concerning Oxehealth were last reviewed in March 2024 (Oxehealth) and May 2024 (EPUT). The Standard Operating Procedure for using the Oxehealth Oxevision and Oxevision Observations was reviewed in May 2024.

2) It's not clear from the response if the DPIA linked to is one or somehow both of DPIA55 and DPIA178, which I requested copies of. Please clarify whether you have provided these DPIAs.

We want to clarify that DPIA178 supersedes DPIA055.

I have attached DPIA055. DPIA178 has recently undergone review and has now been approved. I have attached the current version of DPIA178 and the previous version which has previously been provided.

3) When I requested DPIAs, I expected the information that request covered to include the lawful basis for processing, since identifying this is a requirement of a DPIA. Can you provide this information (the GDPR Article 6 and Article 9 lawful basis for processing) or confirm that you do not hold it?

The legal basis for processing is captured on pages 15 to 18 of the DPIA178 version reviewed in May 2024 (please see the legal basis below).

Article 6 (1) e – “*processing is necessary for the performance of a task carried out in the public interest*”

Article 9 (2) h – “*processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*”

The Standard Operating Procedures (linked to DPIA178) states that;

5.2 Implicit Consent

Oxevision is continually switched on and monitored in every bedroom as part of the safety care plan. Therefore all patients are opted in upon admission as part of the standard ward practice. The patient is encouraged to raise questions and concerns and there are regular opportunities for the patient to engage with staff. Objections can be raised at any time during the admission episode.

However if a patient refuses the use of the Oxevision system in their room, the responsible clinician must be informed. The system is not to be switched off until an MDT meeting within 72 hours has taken place, here the team will decide whether to withdraw the use of the assistive technology if it is in the best interest of the patient, taking into account the balance with individual preference, safety management, mental capacity and other alternatives, just as they would for other treatment approaches. This approach needs to be open and with honest communication including the frequent reiteration of the existence and purpose of the system so staff can be sure that patients informed implicit consent remains in place. If the MDT agrees to switch the system off, the room can be individually isolated with the monitor in the ward base stating 'Camera off'.

The nurse in charge will action the MDT confirmation and ensure that standardised monitoring is in place as per Therapeutic Engagement and Supportive Observations Policy and Procedure CLPG8. The clinical team are to revisit with the patient at agreed intervals the use of this system within their room.

If the MDT decision is to disable a room this must be documented within the patient's record, the care plan must be reviewed and updated and a Datix completed.

Additionally, I requested any DPIAs relating to the use of Oxevision by Trust staff. The DPIA you linked to is explicitly not this: "The processing of data by Essex Partnership University NHS Foundation Trust staff is not in the scope of this DPIA". It also says "It remains the Partner's sole responsibility to conduct a DPIA that meets the requirements of applicable law."

DPIA178, reviewed and updated by EPUT in May 2024, captures the use of Oxevision and Oxevision Observations by EPUT Trust staff. The "Intended Outcomes" includes the following wording;

"Oxevision and Oxevision Observations is implemented to assist in the improvement and recording of quality of care on inpatient wards. The vision-based patient monitoring system provides several features including early warning and alerting of patient vulnerabilities, remote vital sign measurements, and a digital observations functionality for capturing and recording patient observations.

The outcome of these functionalities are to improve patient safety and care."

Linked to DPIA178 is the Standard Operating Procedure for using the Oxehealth Oxevision and Oxevision Observations v10 reviewed in May 2024 which sets out the functionality and use of the system by EPUT staff. A copy has been attached for your review.

4) Please either provide your DPIA that covers the processing of data by Trust staff, or confirm that you do not hold a DPIA that covers the processing of data by Trust staff.

DPIA178, reviewed in May 2024, captures the use of Oxevision and Oxevision Observations by Trust staff.

Publication Scheme:

As part of the Freedom of Information Act all public organisations are required to proactively publish certain classes of information on a Publication Scheme. A publication scheme is a guide to the information that is held by the organisation. EPUT's Publication Scheme is located on its Website at the following link <https://eput.nhs.uk>

Confidential

Oxehealth

Data Protection Impact Assessment

Essex Partnership University NHS Foundation Trust

30 August 2019

Document Control

This document when printed is not authoritative and the latest version location should always be checked.

Author	Simon Hardman, COO, Oxehealth
Document name	Essex Partnership University NHS Foundation Trust – Data Protection Impact Assessment
Latest Version Location	Google Drive / Compliance / DPIA /

Approval Sign-off (For formal issue)			
Owner	Job Title	Date	Version
Simon Hardman	Chief Operating Officer		
Approver	Job Title	Date	Version
Hugh Lloyd-Jukes	Chief Executive Officer, Oxehealth		

Review Panel	
Name	Job Title

Change History			
Version	Date	Author / Editor	Details of Change
1.0		Simon Hardman	First draft version
2.0	29.8.19	Hugh Lloyd-Jukes	Minor evolution to align with SaaS contract reflecting ward pricing and model plus recent use of data by an NHS Trust as part of a Serious Incident Review

1. Introduction

Oxehealth is a spin-out from Oxford University which specialises in novel technology that gives clinicians more time for hands on care where and when they are needed most.

Essex Partnership University NHS Foundation Trust or partner provides provide community health, mental health and learning disability services for a population of approximately 1.3 million people throughout Bedfordshire, Essex, Suffolk and Luton.

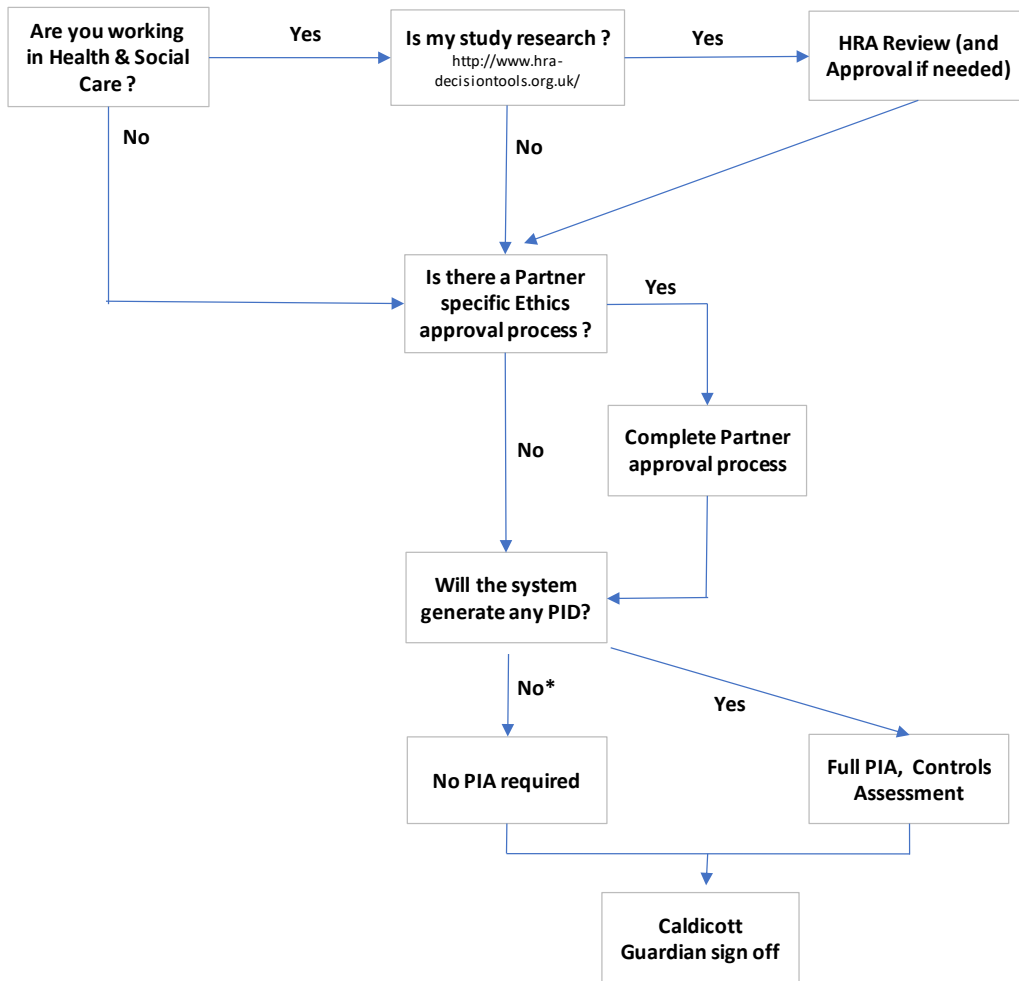
Essex Partnership University NHS Foundation Trust is procuring the following Oxehealth software modules:

- Oxehealth Vital Signs (a Class IIa medical device in Europe)
- Activity Detection for Seclusion
- High Risk Activity Alerts – Dwelling in Bathroom timer and others as developed
- Activity Report

In this project, Essex Partnership University NHS Foundation Trust wishes to deploy the Oxehealth Software & Oxehealth Services to improve and supplement its patient care and safety monitoring regimes.

2. Identification of the need for a DPIA

Before commencing any project with a customer, Oxehealth performs a review of its Compliance Protocol, a simple and specific workflow that steps through the potential questions and decisions points relating to the compliance and approval steps needed prior to commencing work with a customer:



* Note - a PIA is always completed by Oxehealth, required or not

In the case of Essex Partnership University NHS Foundation Trust, the Protocol responses are:

Question	Response	Action Needed
Are you working on Health & Social Care?	Yes	-
Is my study research?	No	-
Are any subjects patients?	Yes	Caldicott Guardian sign off needed
Is there a local, specific approval process	No [tbc with customer]	-
Will the system generate any Personally Identifiable Data?	Yes	Full DPIA and Controls Assessment needed
Are there specific Data Holding requirements?	No [tbc with customer]	-

The screening questions laid out in the Information Commissioner’s Office (ICO) code of practice can also be used as part of the DPIA requirement process:

1. Will the project involve the collection of new information about individuals?

Yes. Whilst CCTV is used throughout Essex Partnership University NHS Foundation Trust facilities and in seclusion rooms, it is not currently used in the patient bedrooms proposed to be used for the project. In this project, digital video cameras will be used to record and process the data to potentially help Essex Partnership University NHS Foundation Trust improve its current patient safety and activity monitoring regimes and, as such, new information about individuals will be collected.

2. Will the project compel individuals to provide information about themselves?

Yes. Given the purpose of the rooms identified for use in the project and the recording of an individual's activity in that room, the individual is compelled to provide information (in the form of video data and the resultant algorithm data and output).

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Yes. Oxehealth staff will have access to non-identifiable algorithm processed data and anonymised video along with short sections of raw video data during the project (for data definitions, see Section 3, Information Flows, below).

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Yes. Oxehealth's software is a novel technology not previously deployed by Essex Partnership University NHS Foundation Trust.

5. Does the project involve you using a new technology which might be perceived as being privacy intrusive?

Whilst CCTV is used throughout Essex Partnership University NHS Foundation Trust facilities and in seclusion rooms, it is not currently used in the patient bedrooms proposed to be used for the project. The use of the new technology might be perceived as being privacy intrusive. However, the opportunity for Essex Partnership University NHS Foundation Trust to improve its current patient safety and activity monitoring regimes is deemed to be a strong reason for the project, provided that appropriate data protection and privacy compliance is ensured.

6. Will the project result in making decisions or taking action against individuals in ways which could have a significant impact on them?

No. Essex Partnership University NHS Foundation Trust wishes to undertake this project with Oxehealth to supplement and support its existing processes.

7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations?

Yes, the project involves video recording of a patient in a room.

8. Will the project require you to contact individuals in ways in which they may find intrusive?

No. There will be no contact at all with individuals involved.

The output of Oxehealth's Compliance Protocol and the answers to the ICO's screening questions clearly indicates the need for a DPIA to be undertaken.

3. Information Flows

A) Types of Information

In this project, almost all the data collected and processed is anonymised and non-personally identifiable (either because the video data is anonymised through techniques such as blurring or because the data is of a mathematical or algorithmic nature). The only exception to this is Salient Video Data - see e) below - which is needed to enable additional investigations to fully debug the system in a specific room or to improve functionality. Only short portions of Salient Video Data (typically up to 10-15 minutes long each) are likely to be collected as part of the project. The collection of this Salient Video Data is driven either by a clinical need (Essex Partnership University NHS Foundation Trust staff identifying something which they wish to bring to the attention of Oxehealth's engineers in order to improve functionality) or the necessity to review an Incident or from algorithmically flagged data which should be reviewed to improve functionality or system performance.

Data is collected from every installation of the Oxehealth software in a room. The equipment used to do this is known as an "Oxeroom" installation with the data stored in a securely encrypted format. This encrypted data is then stored on a server which is not in the Oxeroom but is located nearby on the same site - this is referred to as an "Oxeserver". Finally, some of the data collected is on secure servers.

In this project, the data falls into one of six possible categories:

- a) Anonymised Video Data - Oxehealth will anonymise the camera feed so that the individual is not identifiable from the video. Oxehealth will compress and encrypt this feed and transfer it securely to its secure servers. Anonymised Video Data is required for Oxehealth to debug and improve the Software. The Anonymised Video Data cannot be viewed by unauthorised persons because it is encrypted and – even were it decrypted - the anonymisation prevents the individual being identified (example, see right)



- b) Algorithm Processed Data - 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 Video Data to debug and improve Oxehealth algorithms used in the project. These data are also encrypted and sent to Oxehealth's secure servers. These data cannot identify an individual.
- c) Alert Data - When the algorithm has completed its processing of the camera feed, saving the information to the log file, it extracts room status reports (known as Alert Data, an example of which would be somebody getting out of bed) which are supplied to an output server (known as the User Module). These Alert Data are recorded by the User Module and drive the audible alerts and screen displays. These data cannot identify an individual.
- d) Partner Input Data -The Oxehealth Software enables partner personnel to log their responses to Alerts in the user interface. They can also log or comment on noteworthy events which they would like investigated in the user interface (for example the Software did not Alert to an incident or they observed an incident and would like Oxehealth to examine the algorithm outputs created during it). There is no personal data contained in the Partner Input Data.

- e) Salient Video Data - The Oxehealth Software enables partner personnel to be able to tag time periods during which events of interest to them have occurred and for which they would like to be briefed on the algorithm's performance and potential or which contain an Incident that they wish to review. The raw video for these periods is called Salient Video Data. Salient Video Data which contains staff, patients or other personnel is Personally Identifiable Data.

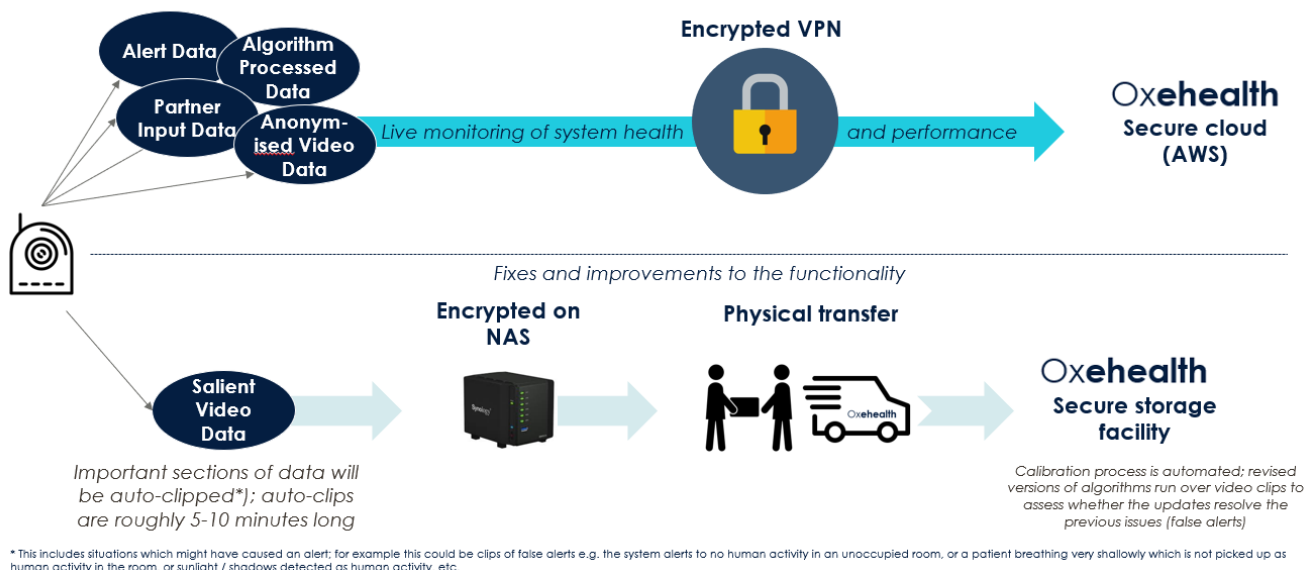
Oxehealth's algorithms or Oxehealth Personnel may also identify Salient Video Data required fully to debug the system or which may present additional interesting insights to the Partner as part of the contract purpose. This data is encrypted and held separately to the Anonymised Video Data and Algorithm Processed Data. Oxehealth will periodically collect the Salient Video Data and transport it by hand to Oxehealth's secure data storage facility (see data journey below).

At least twice per year, Oxehealth provides its partner with a Salient Video Data Report which confirms the purpose, principles and review process for any personally identifiable salient video data collected for the partner and a log of the personally identifiable data retained, reasons for retentions and date of next review. In contrast to Anonymised Video Data, Salient Video Data is encrypted but not anonymised because unanonymised data is required fully to investigate the algorithm's performance (example image, see right). In contrast to Anonymised Video Data, Salient Video Data will be short episodes (typically up to 10-15 minutes in length) so the total volume of video is expected to be low



- f) Oxehealth Data Annotations - Oxehealth staff may create notes and other commentaries (known as Oxehealth Data Annotations) relating to Salient Data, Anonymised Data, Algorithm Processed Data, Partner Input Data or Alert Data. There is no personal data contained in the Oxehealth Data Annotations.

B) The Data Journey



Data will be collected from every Oxeroom installation and is transferred, in an encrypted format via Ethernet cabling, to the Oxeserver, located in an office within the secure partner facility. From the Oxeserver, data travels to Oxehealth via two mediums - over the internet and by the physical movement of storage devices by Oxehealth staff.

a) Data that travels to Oxehealth via the Internet (over encrypted connection)

Oxehealth will collect various data (Anonymised Video Data, Algorithm Processed Data, Alert Data and Partner Input Data) that allows the company to monitor and improve the system.

Data travels using a secure connection (encrypted) from the on-site Oxeserver to secure Oxehealth servers. None of this data is personal data (see above).

b) Data that arrives at Oxehealth via the physical movement of storage devices

Salient 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 on a regular basis, with the devices physically being transferred to Oxehealth’s secure data storage facility. During this transfer process Oxehealth staff (or a delegated secure courier) 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.

Oxehealth Data Annotations are created on secure, access-controlled servers and do not contain any personal data.

C) Usage of data at Oxehealth

As set out above, the vast majority of data used in the project is not personal and so is out of the scope of this DPIA. Any data retained on secure Oxehealth servers will only be used for the contract purpose – the

deployment of the Oxehealth Software & Oxehealth Services by Essex Partnership University NHS Foundation Trust to improve and supplement its patient care and safety monitoring regimes [check to Contract Purpose].

Much of the data analysis will be performed automatically, using computers, over salient and anonymised data for the contract purpose. For example, running a new version of algorithms across all video data in order to quantify the time for which vital signs were estimated when the room was occupied. This process is done without viewing the data and engineers will simply gain access to summary statistics at the end of this process.

From time to time, Oxehealth's engineers may need to review a short period of salient data to understand why certain system outputs are being generated or are failing to be generated – these short periods will only be viewed by Oxehealth staff.

Oxehealth retains salient video data in order to improve algorithm performance, specifically:

1. To reduce the false alert rate.
2. To reduce the risk of true alerts being suppressed.
3. To prevent performance regression or overfitting of upgraded algorithms.

Oxehealth also retains data at the request of Essex Partnership University NHS Foundation Trust, should events of interest to them occur for which they require salient video data to be securely stored for future use by Essex Partnership University NHS Foundation Trust.

As part of this analysis, annotations may be added by an engineer, to:

- Identify data of a sensitive nature and moving this to a separate stored location with access restricted to senior management of Oxehealth
- Identify data of a potentially distressing, but not sensitive, nature so this is flagged up to a user before reviewing
- Record room occupancy status and timing
- Record patient activity generating algorithmically interesting data
- Identifying algorithm issues which need investigating.

No copies of the data will be created for this and no still images will be taken. The data will be accessed directly from the server.

All staff with access to the data will 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 patient identifiable video data will be used for marketing, or publicity purposes.

Oxehealth undertakes periodic reviews with the Partner to consider the salient video data held, the reason for the data retention and confirmation of salient data deleted.

D) Data security

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 partner information assets). Amongst the many controls in place, Oxehealth's storage servers are within a secure facility which 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.

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). Staff use different sets of credentials for Virtual Private Network (VPN), remote machine access and fileserver access. Staff VPN access is granted to selected staff and is audited. Logging and pattern-based alerts are active on the firewall and VPN. The system and network are subject to regular Penetration Testing by certified third party information security specialists.

Whilst the data is being recorded it will be stored on the local compute equipment in the secure housing (Oxecam) or securely at Essex Partnership University NHS Foundation Trust (Oxeserver). Any data transfer over the internet will be in encrypted format. During transfer of the data back to Oxehealth's secure facility the servers will be accompanied at all times by a member of the Oxehealth team or a secure courier.

4. Privacy and related risks

An assessment of the proposed project identified the following potential risks in relation to the privacy of an individual:

Risk ID	Privacy Issue	Risk to the individual	Compliance Risk	Organisational Risk
1	Data disclosed inadvertently to a third party or data is lost.	The video data could become public.	GDPR Principle 6	Risk of negative publicity (to Oxehealth and Essex Partnership University NHS Foundation Trust) due to incomplete information being given about the desire to improve the safety of patients. Appearance of poor data protection compliance and associated ICO fines.
2	Unnecessary intrusion into a patient's privacy	The video data could become public. People external to Essex Partnership University NHS Foundation Trust become aware of a patient's use of a room.	GDPR Principle 6	Risk of negative publicity (to Oxehealth and Essex Partnership University NHS Foundation Trust) due to incomplete information being given about the desire to improve the safety of patients. Appearance of poor data protection compliance and associated ICO fines.
3	Identification of a patient by an Oxehealth staff member	The video data could become public.	GDPR Principle 6	Distress to Oxehealth staff by identifying someone known to them.
4	Data retained longer than necessary	Data pertaining to a patient is retained longer than required.	GDPR Principles 2 and 5	Risk of data being used for purposes beyond the original purpose. Appearance of poor data protection compliance and associated ICO fines.
5	Patient unaware their data is being collected	The patient is unaware of their rights under the General Data Protection Regulations (GDPR)	GDPR Principles 1, 3 and 6	Risk of negative publicity (to Oxehealth and Essex Partnership University NHS Foundation Trust) due to incomplete information being given about the desire to improve the safety of patients. Appearance of poor data protection compliance and associated ICO fines.
6	Data moved to another country with different data protection	Reduced protection on rights and freedoms of data subjects.	GDPR Article 45	Risk of data being used for purposes beyond the original purpose.

	rules			Appearance of poor data protection compliance and associated ICO fines.
--	-------	--	--	---

5. Proposed Privacy Solutions

Following the identification of the potential risks in Section 4, a range of proposed solutions will be used to mitigate and control these risks. These are as follows:

Risk 1 – Data disclosed inadvertently to a third party or data is lost

Essex Partnership University NHS Foundation Trust already have strict practices surrounding data confidentiality and privacy of patients, governed by the NHS Code of Confidentiality and the Caldicott Principles. No additional personally identifiable data will be made available to Essex Partnership University NHS Foundation Trust staff as a result of this project.

The Oxeserver will be located securely at Essex Partnership University NHS Foundation Trust with physical and electronic access restricted to authorised Essex Partnership University NHS Foundation Trust or Oxehealth personnel. Essex Partnership University NHS Foundation Trust staff are bound contractually by the Caldicott Principles and the NHS Code of Confidentiality. In addition, the video data held on Oxecam or an Oxeserver 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 Essex Partnership University NHS Foundation Trust staff is therefore deemed to be very low.

To avoid a potential data leak due to theft or malicious electronic attack (and therefore mitigate the risk of accidental damage to or loss of data), Oxehealth have 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 Oxecam, and the data contained therein, is held in a secure housing in a room and the Oxeserver is within a secure area at Essex Partnership University NHS Foundation Trust
- Portable storage devices are always accompanied in transit by Oxehealth staff or a secure courier
- Salient Video Data storage is in a secure room with limited keyholder access in a building with 24-hour security guards. This is backed up at Oxehealth, until secure deletion, onto secure tapes held offline in a secure, fire-resistant environment
- 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 file servers are only accessible from the Oxehealth IP range, using individual logons only
- All data collected and generated by the Oxehealth system is anonymised and therefore not personally identifiable. The only exception to this is Salient Video Data (which includes raw video data and is needed to fully debug the system or enable additional research to improve functionality). In addition to the above measures, to manage any further potential risk from Salient Video Data:
 - The data is securely encrypted
 - It is held separately from the Anonymised Video Data and Algorithm Processed Data
 - Access to Salient Video Data requires authorisation by a member of the Oxehealth Leadership Team

Risk 2 – Unnecessary intrusion into a patient’s privacy

As identified in Section 2 of this assessment, the nature of this project means that video recording of patients is undertaken. However, CCTV is in place already at Essex Partnership University NHS Foundation Trust and used extensively throughout the facility. The Oxehealth Software solutions are being developed to improve the current patient safety and care regimes of Essex Partnership University NHS Foundation Trust.

As discussed above, all data collected and generated by the Oxehealth system is anonymised and therefore not personally identifiable. The only exception to this is Salient Video Data (which includes raw video data and is needed to fully debug the system or enable additional research to improve functionality). The use of Salient Video Data is kept to a minimum, used only when Essex Partnership University NHS Foundation Trust want to bring something to the attention of Oxehealth in order to improve functionality or Oxehealth’s researchers identify sections of interest to be analysed). At no point do Oxehealth staff have access to patient names, medical history or reason for being in the hospital.

Risk 3 – Identification of a patient by an Oxehealth member of staff

All data collected and generated by the Oxehealth system is anonymised and therefore not personally identifiable except for the Salient Video Data (which is only used minimally as explained above).

For Salient Video Data, there is a low risk of Oxehealth staff being able to identify patients from the video data, given the small number of patients involved and the limited number of Oxehealth people able to review this Salient Data. The risk of identification cannot be ruled out but is considered to be relatively low – in addition, Oxehealth staff are bound by its detailed code of conduct concerning the use and security of patient data.

In the event of a member of the Oxehealth team being able to identify a patient involved in the project, all data relating to that patient would be deleted.

Risk 4 – Data is retained longer than necessary

In the project, Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust (unless applicable law prevents Oxehealth from doing so).

All data collected and generated by the Oxehealth system is anonymised and therefore not personally identifiable - as the data is not personally identifiable, it can be kept by Oxehealth.

The exception to this is Salient Video Data (which is only used minimally as explained above in Risk 2). The Salient Video Data will only be kept for as long as is needed to answer queries raised by Essex Partnership University NHS Foundation Trust staff or by researchers at Oxehealth. To support this, all data files are date and time stamped so that retention can be tracked, reviews of data stored are undertaken regularly and the data will be securely deleted at the end of the project or when no longer required, whichever is the earlier.

Risk 5 – Patient is unaware their data is being collected

Patients in the proposed rooms of Essex Partnership University NHS Foundation Trust are in the care of expert and highly trained Essex Partnership University NHS Foundation Trust staff who will take decisions in the best

interest of those patients. Essex Partnership University NHS Foundation Trust will maintain a regime that informs patients in an appropriate fashion.

Risk 6 – Data is moved to another country with different data protection rules

As explained above, only minimal personally identifiable data (Salient Video Data) will be retained as part of the project and this will only be retained for the minimum time necessary to allow conclusion of research by Oxehealth to develop further functionality or to respond to queries by Essex Partnership University NHS Foundation Trust staff.

This data is stored physically on secure servers in the UK and Oxehealth has no intention of moving its business, or this data, outside of the UK. In the unlikely event of Oxehealth moving its business out of the UK, the data would be retained within the UK and therefore under its data protection regime.

6. DPIA Outcomes

The partnership being proposed between Oxehealth and Essex Partnership University NHS Foundation Trust has the potential to drive improvement in patient safety and care regimes.

Whilst a successful outcome of this nature is desired for the project, the primary focus for Oxehealth and Essex Partnership University NHS Foundation Trust is to ensure respect for the patient and their privacy at all times and that any data generated during the project is processed, transferred, stored or reviewed in a safe and timely manner that complies with Data Protection legislation and the Caldicott Principles.

A thorough assessment of the potential risks which might impact a patient’s privacy has been undertaken as well as a detailed review of all data flows and usage in the project. For each risk, a range of proposed solutions has been identified in Section 5 of this DPIA, and it is recommended that each of these be implemented to ensure a successful outcome for the project in terms of patient privacy and data compliance.

Recommended by: 

Date:

Simon Hardman
COO, Oxehealth Limited

DPIA Approval: 

Date:

Hugh Lloyd-Jukes

CEO, Oxehealth Limited

Approved by: Mark Madden - Senior Information Risk Owner (SIRO)

Essex Partnership University NHS Foundation Trust (EPUT)

A handwritten signature in black ink, appearing to read 'Mark Madden', is positioned above the 'Signed:' text.

Signed:

Date: 02.10.19

Appendix 1

General Data Protection Regulations Principles and Oxehealth's Compliance [Boxed responses]

Source: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/>

Personal data shall be:

1. **processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness,**

There must be legitimate grounds for collecting personally identifiable data and it must not have a negative effect on a data subject or be used in a way they wouldn't expect – We are aware that recording people can impact their privacy. It is important that any potential infringement on an individual's privacy be in pursuit of a legitimate aim and be proportionate. We consider healthcare and protection of law and order to be legitimate aims for this purpose. It will not always be necessary to obtain an individual's consent to a course of action that affects their privacy, for example, if the system is used in the normal course of treatment. In line with the Mental Capacity Act it may be that an advocate or the subject's clinical team are able to provide appropriate consents in situations where consent is deemed necessary. We recommend our customers place signage notifying data subjects of the use of the technology.

fairness and transparency');

2. **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');**

Data should be collected for specified and explicit purposes and not be used in a way someone wouldn't expect – The purpose for which the Oxehealth system is being used by a customer is clearly and transparency laid out in the contract between Oxehealth and that customer; this Data Protection Impact Assessment sets out the controls and processes implemented by Oxehealth to ensure data processing is only undertaken in a way compatible with this purpose.

All data collected and processed as part of this project is anonymised and non-personally identifiable. The only exception is Salient Video Data which is needed to fully debug the system or enable additional investigations to improve project functionality. The use of Salient Video Data is kept to a minimum, used only when partner wants to bring something to the attention of Oxehealth in order to improve functionality or Oxehealth's engineers identify sections requiring analysis. At no point do Oxehealth staff have access to patient names, medical history or reason for being in the room.

3. **adequate, relevant and limited to what is necessary in relation to the purposes for which they are**

As per 2 above, the only data collected that is personally identifiable is Salient Video Data. The collection of this is kept to a minimum and only used in order to fully debug the system or enable additional investigation to improve project functionality. Salient Video Data is deleted once these tasks have been fully completed.

processed ('data minimisation');

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are

It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected – as per 2 above, the only data collected that is personally identifiable is Salient Video Data. The collection of this is kept to a minimum and only used in order to fully debug the system or enable additional investigations to improve project functionality.

erased or rectified without delay ('accuracy');

5. 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; ('storage limitation');

As per 2 above, the only data collected that is personally identifiable is Salient Video Data in which a person appears. This is reviewed only in order to fully debug the system or enable additional investigations to improve project functionality. No changes to the raw video data are made therefore the personal data is accurate and unchanged from when it is collected.

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using

Non-compliance with Principle 6 is a key risk for Oxehealth with full details of the approach taken to compliance laid out in Sections 3D and 5 of the DPIA.

appropriate technical or organisational measures ('integrity and confidentiality').



Data Protection Impact Assessment (DPIA)

Introduction

A [data protection impact assessment \(DPIA\)](#) will help you to identify and mitigate potential data protection risks to an acceptable level before using or sharing (processing) data that identifies individuals (personal data).

A DPIA will also help you meet a number of data protection legal requirements including:

- [Data protection by design](#) - privacy and data protection issues must be considered at the start, or in the design phase, of a new system, product or process, then continuously while it exists.
- [Accountability](#) - your organisation is responsible for showing how it complies with data protection laws.
- [Transparency](#) - personal data must be used and shared in a transparent way.
- [Security](#) - adequate measures need to be in place to protect data. This can range from policies and procedures to technical security measures such as encryption of data.

DPIAs are mandatory when there is a high risk to individuals, such as when using the health and care data of a large number of people. However, health and care organisations are strongly advised to complete a DPIA when using and sharing personal data in a new or substantially changed way.

A DPIA involves a risk assessment. If a high-level risk remains after applying mitigations, then you must consult with the Information Commissioner's Office (ICO) for further advice before starting to collect, use or share the data.

A DPIA is a live document - you must update it if there are any changes to:

- the purpose - why you are proposing to use or share personal data
- the manner - how you will use or share the data
- who is involved - the organisations using and sharing personal data

In the case of research, the sponsor is the controller.



Essex Partnership University

NHS Foundation Trust

See Health Research Authority (HRA) guidance on [controllers](#) and research. HRA guidance on [DPIAs](#) sets out that sponsors should complete a DPIA for the broad range of health and care research they sponsor and ensure that individual research projects are designed in accordance with the DPIA.

Individual DPIAs should only need to be completed for individual research projects that involve activities beyond the generic research DPIA. Where the study deviates from the established processes (for example, where it is intended that a project uses a new technology for the processing of personal data, or requires that safeguards set out in standing policies cannot be applied), the sponsor should consider whether a study specific DPIA is appropriate to address the level of risk, or whether updating existing DPIA(s) will be sufficient. Research sites should not complete DPIAs or request researchers to complete individual DPIAs for each research project, as they are not the controller.

Text in **square brackets and green highlight** is guidance and should be removed for the final version.

Text in **yellow highlight** is sample wording and should be edited according to your local circumstances.

Timescales for completion of a DPIA

Action	Timescale
Template sent to Project Lead for completion & return to IG Team	N/A
Advice & recommendations returned to Project Lead for updating	+ 1 week (for each required event repeated as necessary)
Basic service/project updates completed	Move to approvals
DPIA confirms no person identifiable / corporately sensitive data involved / no impact on Trust	IG Manager Approval (if no other input required) +1 week.



Patient identifiable data involved / Person identifiable / corporately sensitive data involved / impact on Trust	+ 1 Month (where further input from DPO/Cyber/Projects/Contracts/PMO is required for each required event +1 week repeated as necessary)
Final approval (including further questions from SIRO)	+ 1 Month (SIRO Approval for each required event +1 week repeated as necessary)
Unplanned events (Delays/projects on hold/no response/tracking required stakeholders)	Delays will cause DPIA to be archived into a draft folder/no longer required folder. <i>IG are not responsible for chasing completion of DPIA's outside of our process (only exception - final approval /sign off).</i>

Project Info

This is where the project / system / service is described to us –

We need to know what you want to do, why and what the outcomes would be.

We also need to know what organisations are involved.

If the project / system / service has previously had a DPIA carried out and this is regarding a change to the project / system / service - please get in touch with the IG team as we may be able to use or modify the previous assessment - this will be highlighted as you fill in this section.



Essex Partnership University

NHS Foundation Trust

Stage 1

This is where the personal information elements of the project / system / service are described to us.

If any of the questions are answered "Yes", then a full Stage 2 PIA will need to be carried out.

Stage 2


Please provide as much information as possible in answer to the questions. You may need to request the answers to some of the questions from the system supplier / provider.

Please see the glossary which you can refer to in order to assist you with completion, alternatively you can request assistance from the IG team.

Please return this form or contact us for support on Epunft.dpia@nhs.net

Project Overview

Reference number (to be assigned by IG team)	DPIA178		
Organisations involved - If multiple, please indicate the lead / host Organisation with (lead) following the name.	EPUT	Oxehealth	
Project Name	Oxevision (Business As Usual)		
Project Outline (Purpose)	<p>Oxevision is active on numerous inpatient wards with a goal of installation on all remaining qualified ward. Oxevision is a contact-free system that can be used by staff to help improve patient safety and experience on the ward. It is designed to give staff the insights they need to plan patient care and intervene proactively.</p> <p>Oxevision uses an infrared sensitive camera housed in a secure, anti-ligature housing unit which is positioned between the ceiling and the wall in the patient's room.</p>		

	<p>The outputs from this camera are analysed digitally using specially developed algorithms to provide staff with alerts, readings, and reports via a screen in the nursing station and dedicated tablets for when they are moving around the ward. These alerts, readings, and reports help staff to ensure patients and care home residents remain safe and secure.</p> <p>Oxevision Observations is an added module to Oxevision. It is a tool designed to digitise observation rounds and work alongside existing processes, helping to reduce the need for paper-based methods and improve patient observation and engagement.</p>
<p>Intended Outcomes (what they are trying to achieve)</p>	<p>Oxevision and Oxevision Observations is implemented to assist in the improvement and recording of quality of care on inpatient wards. The vision-based patient monitoring system provides several features including early warning and alerting of patient vulnerabilities, remote vital sign measurements, and a digital observations functionality for capturing and recording patient observations.</p> <p>The outcome of these functionalities are to improve patient safety and care.</p> <div style="text-align: center;">  </div> <p>DPIA - Oxevision with Oxevision Observati</p>
<p>Proposed Implementation Date</p>	<p>Currently in place</p>



Essex Partnership University

NHS Foundation Trust

Responsible lead(s)	Name	Vijay Chuttoo	Lianne Joyce
	Job title	Deputy Director for Quality and Safety, Specialist Services	Deputy Director Quality & Safety
	Email	vijay.chuttoo@nhs.net	lianne.joyce2@nhs.net
Individual completing DPIA If different from responsible lead	Name	Derrick Trimble	
	Job title	Oxevision System Manager (Interim)	
	Email	Derrick.trimble1@nhs.net	
Key Stakeholders (list / or individual role or title or name)	All ward managers, Legal Team, DPO Office, IG Team, IT Department, Senior Management, Oxevision, Police, Coroners Office, Inquest Team, Lawyers		
Is there a project plan in place? If so, please supply	Each implementation has a project plan		

STAGE 1

Screening Questions		Yes/No
Q1	Is this relating to a change to an existing system, service or process?	Yes
Q2	Will the process, service or system include the processing ^[1] of personal ^[2] or sensitive ^[3] information?	Yes
Q3	Will the process, service or system involve the collection of new information about individuals?	Yes
Q4	Will the process, service or system compel individuals to provide information about themselves?	No
Q5	Will personal information be released/shared with organisations or people who have not previously had access to the information?	Yes
Q6	Are you using the information for a different purpose than originally agreed or communicated to the data subject?	No
Q7	Does the process or system involve the use of new technology that might be perceived as being privacy-invasive? (i.e. biometrics, cookies, finger print identification, IP Addresses etc.)	Yes



Essex Partnership University

NHS Foundation Trust

Q8	Will the project result in you making decisions or taking action against individuals in ways, which could have a significant impact on them - positive or negative? (i.e. service planning, commissioning of new services)	Yes
Q9	Is the information about individuals likely to raise privacy concerns or expectations? (The project will use pseudonymised data about the individuals)	Yes
Q10	Will the process or system require you to contact individuals in ways, that they may find intrusive?	Yes
Q11	Has this process or system already started as a pilot without a DPIA being undertaken?	No
Q12	Has this process or system already had a DPIA undertaken?	Yes

[1] Processing: obtaining, recording or holding the information or data, carrying out any operation or a set of operations on the information or data.

[2] Examples of Personal Data (any information related to a natural person that can be used to identify the person): name, address, date of birth, postcode, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

[3] Examples of Sensitive / Special Category Data that are subject to additional protections: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.



Section 1. WHAT DATA DO YOU WANT TO USE OR SHARE?

Can you use anonymous data for your purposes? If not, explain why.

Put an [x] next to the one that applies.

<input type="checkbox"/>	Yes
<input checked="" type="checkbox"/>	No
<input type="checkbox"/>	Unsure – try to provide an explanation of what you think

The Oxevision system identifies use of the system by room numbers or room identification but there is an image of the person within the room. There is no personal identification data captured by the Oxevision system other than the image of the person. Vital signs, clear or anonymised video data can be viewed or collected but does not have associated personal identification data within the Oxevision system.

The Oxevision Observation functionality is integrated at the user-end with EPUT patient summary data (PSD). This enables staff to record vital sign and observation data associated with a specific patient The data is processed through the Oxevision system but remains encrypted throughout the process until it is consumed by the end-user at the Trust. Oxehealth staff do not have access to encrypted data or patient specific data.

1. Which types of personal data do you need to use and why?

Put an [x] next to all that apply.

x	Forename		Physical description, for example height		Photograph / pictures of people
x	Surname		Phone number	X	Location data e.g. <ul style="list-style-type: none"> • Other – Ward name and room number



Essex Partnership University

NHS Foundation Trust

	Address		Email address		Audio recordings
	Postcode full		GP details	x	Video recordings The Oxevision system is a vision-based patient monitoring system with a camera installed. Clear video data is available upon the selection of the take vital signs option. Clear video data (CVD) is retained on the local server on a 24 hour cycle. CVD data may be requested by the Trust which will be collected by Oxehealth staff from the server and delivered on a cloud based strategy to provide our clear video data.
	Postcode partial		Legal representative name (personal representative)		Other
x	Date of birth	x	NHS number		None
x	Age		National insurance number		
x	Gender	x	Other numerical identifier – Paris ID and Hospital ID		

The data is required from the patient summary record to assign patients to the Oxevision Observation dashboard and produce subsequent observation reports for uploading to the respective electronic patient record system.

The output data is a replication of the paper-based observation sheets in CLP8. The data is used exactly as a typically scanned document: uploaded to the respective EPR, accessed by the EPR, and managed within the context of the EPR.

2. Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Data that relates to criminal offences is also considered particularly sensitive. Which types of sensitive data do you need to use or share?

Put an [x] next to all that apply.

Type of data		Reason why this is needed (leave blank if not applicable)
[x]	Information relating to an individual's physical or mental health or condition, for example information from health and care records	Data recorded in Oxevision Observations are entries made by ward staff conducting levels 1 – 4 observations. Any patient oriented information notable for the relative observation level is, or should be, recorded. The digital recording of observations in Oxevision Observations replaces paper-based observation records. . In Oxevision, data is only displayed as a room number. No identifiable patient is displayed on the system when not being used for Oxevision Observations.
[x]	Biometric information in order to uniquely identify an individual, for example facial recognition	Vital Sign data collected from patients using Oxevision are used in providing patient care and assessing trends in physical health.
[]	Genetic data, for example details about a DNA sample taken as part of a genetic clinical service	
[]	Information relating to an individual's sexual life or sexual orientation	



<input type="checkbox"/>		
<input type="checkbox"/>	Racial or ethnic origin	
<input type="checkbox"/>	Political opinions	
<input type="checkbox"/>	Religious or philosophical beliefs	
<input type="checkbox"/>	Trade union membership	
<input type="checkbox"/>	Information relating to criminal or suspected criminal offences	
<input type="checkbox"/>	None of the above	

Data Set for Oxevision Observations

----- EPUT-TO-OXE -----

Patient list - (all current inpatients from Mobius/Paris)

- LocalID (hospital number)
- NHS#
- Dob
- Fname, Lname
- Gender
- TraceCode

----- OXE-TO-EPUT -----

PatConfig - (will contain "dateEffective", plus at least one of the below)



- DateEffective
- Obs Level A
 - Level
 - TimeOfDay
 - LocationApplicable
 - reasons
- Obs Level B
 - Level
 - TimeOfDay
 - LocationApplicable
 - Reasons
- Notes
- CurrentRoom
- RiskFactors

ObsCluster

- DateTime
- LocationType
- Ward
- ObserverName
- ObsTakenUnderLevel (eg patient could be assigned to obs level 1, but an observation may be taken under level 2)
- Intervention
- Engagement
- Presentation
- Breathing Rate
- Heart Rate

3. Who are the individuals that can be identified from the data?

Put an [x] next to all that apply.

<input checked="" type="checkbox"/> Patients or service users
<input type="checkbox"/> Carers
<input checked="" type="checkbox"/> Staff – Those staff that take observations are identified as the assigned observers



<input type="checkbox"/> Wider workforce
<input type="checkbox"/> Visitors
<input type="checkbox"/> Members of the public
<input type="checkbox"/> Other -

4. Where will your data come from?

Data is collected on two paths:

Oxevision

Oxevision monitors patient activity in the room through an optical array that includes a camera, infrared light, and staff interfaces (tablet or monitor).

Oxevision Observations

For Oxevision, data comes from two sources: The patient summary data is referenced from the Trust PSD server. The data is not exposed to Oxehealth or an external organisation. The PSD data is essential for staff to assign a patient to a room where Oxevision Observations can be recorded. The primary collection of patient data is relative to observations conducted by staff and becomes part of the Document of Record in the respective EPR.

5. Will you be linking any data together?

Put an [x] next to the one that applies.

<input checked="" type="checkbox"/> Yes – provide an explanation below and then go to 5a
<input type="checkbox"/> No – skip to question 6
<input type="checkbox"/> Unsure – try to provide an explanation of what you think then go to question 5a



Essex Partnership University

NHS Foundation Trust

- a. Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?

Put an [x] next to the one that applies.

<input checked="" type="checkbox"/> Yes – [provide details below]
<input type="checkbox"/> No
<input type="checkbox"/> Unsure – [try to provide details below]

Where data is linked is where the PSD populates the OxeObs dashboard with patient-identifiable information. There is no other linkage.

Section 2. WHERE WILL DATA FLOW?

6. Describe the flows of data.

Data flow name	Going from	Going to	Data description
Room number	Oxevision system	Oxevision system and reports	Information relative to a room is used in all reporting. There is no patient identification in the Oxevision system.
Patient room assignment	PSD	Oxevision Observation Dashboard	PSD data is essential to assign a patient to a room for conducting observations.

7. Confirm that your organisation's information asset register (IAR), record of processing activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.

Put an [x] next to the one that applies.



Essex Partnership University

NHS Foundation Trust

<input checked="" type="checkbox"/> Yes
<input type="checkbox"/> No
<input type="checkbox"/> Unsure - add as a risk with an action to find out

8. Will any data be shared outside of the UK?

Put an [x] next to the one that applies.

<input type="checkbox"/> Yes - go to question 8a
<input checked="" type="checkbox"/> No - skip to question 9
<input type="checkbox"/> Unsure - add as a risk with an action to find out then skip to question 9

- a. If yes, give details, including any safeguards or measures put in place to protect the data whilst outside of the UK.

Section 3. IS THE INTENDED USE OF THE DATA LAWFUL?

9. Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?

The list below contains the most likely conditions applicable to health and care services.
Put an [x] next to the one that applies.

<input type="checkbox"/> (a) We have <u>consent</u> - this must be freely given, specific, informed and unambiguous. It is not appropriate to rely on consent for individual care or research, even if you have obtained consent for other reasons, but is likely to be needed for the use of cookies on a website.
--



Essex Partnership University

NHS Foundation Trust

<input type="checkbox"/> (b) We have a contractual obligation - between a person and a service, such as a service user and privately funded care home.
<input type="checkbox"/> (c) We have a legal obligation - the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.
<input checked="" type="checkbox"/> (e) We need it to perform a public task - a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.
<input type="checkbox"/> (f) We have a legitimate interest - for example, a private care provider making attempts to resolve an outstanding debt for one of its service users. This cannot be relied on by public bodies in the performance of their tasks.
<input type="checkbox"/> Other – The standard operating procedures details a process for ensuring patient are informed on how to submit an objection or restriction to the processing of their data.

10. If you have indicated in question 2 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?

The list below contains the most likely conditions applicable to health and care services. Put an [x] next to the one that applies.

<input type="checkbox"/> (b) We need it to comply with our legal obligations for employment - for example, to check a person's eligibility to work in the NHS or a local authority. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.
<input type="checkbox"/> (f) We need it for legal claims, to seek legal advice or judicial acts - the information is required to exercise, enforce or defend a legal right or claim, for example a person bringing litigation against a health or care organisation.
<input type="checkbox"/> (g) We need to comply with our legal obligations to provide information where there is a substantial public interest, as set out in this list - for example, safeguarding of children and individuals at risk.



Essex Partnership University

NHS Foundation Trust

<input checked="" type="checkbox"/> (h) We need it to comply with our legal obligations to provide or manage health or social care services - providing health and care to a person, or ensuring health and care systems function to enable care to be provided. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.
<input type="checkbox"/> (i) We need it to comply with our legal obligations for public health - using and sharing information is necessary to deal with threats to public health or to take action in response to a public health emergency (such as a vaccination programme). See Annex 2 for the most likely laws that apply when using and sharing information in health and care.
<input type="checkbox"/> (j) We need it for archiving, research and statistics where this is in the public interest - for example, health and care research, with relevant safeguards in place for the use of the participant's health and care information. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.
<input type="checkbox"/> Other
<input type="checkbox"/> Not applicable - the use of special category data is not proposed

11. What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?

Patient data is not shared with external organisations or persons. Implied consent of the service user for use of Oxevision is described in the [standard operating procedures](#).

Put an [x] next to the one that applies.

<input checked="" type="checkbox"/> Implied consent - for individual care or local clinical or care audits - skip to question 12.
<input type="checkbox"/> Legal requirement - this includes where NHS England has directed an organisation to share the data using its legal powers. State the legal requirement in the further information section. Go to question 11a.
<input type="checkbox"/> Section 251 support - this means you have support from the Secretary of State for Health and Care or the Health Research Authority following an application to the Confidentiality Advisory Group (CAG). CAG must be satisfied that it isn't possible or practical to seek consent. Go to question 11a.
<input type="checkbox"/> Overriding public interest - for example to prevent or detect a serious crime or to prevent serious harm to another person. The justification to disclose must be balanced against the public interest in maintaining public confidence in health



Essex Partnership University

NHS Foundation Trust

and care services. Routine use of this is extremely rare in health and care, as it usually applies to individual cases where decisions are made to share data. Go to question 11a.

Not applicable - we are not proposing to use identifiable health and care data. Skip to question 12.

a. Please provide further information or evidence.

Provide evidence as follows depending on your selection in question 11:

(From v 9.1 [standard operating procedures](#).)

5.2 Implicit Consent

Oxevision is continually switched on and monitored in every bedroom as part of the safety care plan. Therefore all patients are opted in upon admission as part of the standard ward practice. The patient is encouraged to raise questions and concerns and there are regular opportunities for the patient to engage with staff. Objections can be raised at any time during the admission episode.

However if a patient refuses the use of the Oxevision system in their room, the responsible clinician must be informed. The system is not to be switched off until an MDT meeting within 72 hours has taken place, here the team will decide whether to withdraw the use of the assistive technology if it is in the best interest of the patient, taking into account the balance with individual preference, safety management, mental capacity and other alternatives, just as they would for other treatment approaches. This approach needs to be open and with honest communication including the frequent reiteration of the existence and purpose of the system so staff can be sure that patients informed implicit consent remains in place. If the MDT agrees to switch the system off, the room can be individually isolated with the monitor in the ward base stating 'Camera off'.

The nurse in charge will action the MDT confirmation and ensure that standardised monitoring is in place as per Therapeutic Engagement and Supportive Observations Policy and Procedure CLPG8. The clinical team are to revisit with the patient at agreed intervals the use of this system within their room.



If the MDT decision is to disable a room this must be documented within the patient's record, the care plan must be reviewed and updated and a Datix completed.

Section 4. HOW ARE YOU KEEPING THE DATA SECURE?

12. Are you collecting information?

Put an [x] next to the one that applies.

Yes - go to question 12a

No - skip to question 13

a. How is the data being collected?

- Direct entry of data into Oxevision Observations.
- Room activity per Oxevision system logs
- Clear Video Data collected via a cloud based strategy to provide our clear video data

13. Are you storing information?

Put an [x] next to the one that applies.

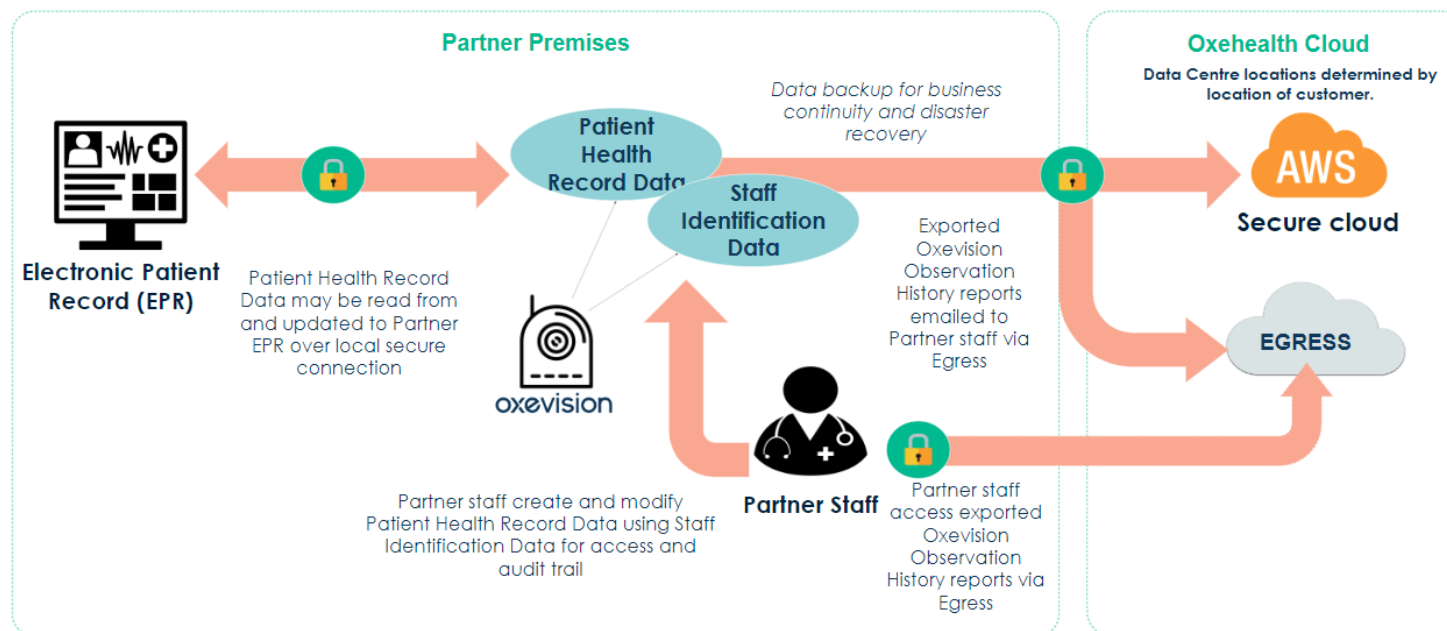
Yes – go to question 13a

No – skip to question 14

a. How will information be stored?

Put an [x] next to all that apply.

<input type="checkbox"/>	Physical storage, for example filing cabinets, archive rooms etc
<input checked="" type="checkbox"/>	Local organisation servers
<input checked="" type="checkbox"/>	Cloud storage – Amazon Web Services (AWS). Specifics provided in supplier DPIA support document
<input type="checkbox"/>	Other



Data Flows from the Partner Electronic Patient Record (EPR) and the Oxevision Observations software on Partner Premises to Oxehealth

14. Are you transferring information?

Put an [x] next to the one that applies.

Yes – go to question 14a

No – skip to question 15

a. How will information be transferred?

We use a cloud-based strategy to provide clear video data.



CVD Delivery via
Egress v1.0.pptx

15. How will you ensure that information is safe and secure?

All data generated by the Oxevision system is stored on local secure servers at EPUT Oxevision deployed sites.

Some data (AVD, APD, UIOD, SID and PHRD) is 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.

Put an [x] next to all that apply.

Encryption

Password protection

Role based access controls (RBAC) – where users only have access to the data held digitally which is needed for their role (this includes setting folder permissions)



Essex Partnership University

NHS Foundation Trust

<input checked="" type="checkbox"/> Restricted physical access – where access to personal data is restricted to a small number of people, such as access cards or keys to a restricted area
<input checked="" type="checkbox"/> Business continuity plans
<input type="checkbox"/> Other

16. How will you ensure the information will not be used for any other purposes?

Specify the measures below which will be used to limit the purposes the data is used for.

Put an [x] next to all that apply and provide details.

<input checked="" type="checkbox"/> Contract
<input type="checkbox"/> Data processing agreement
<input type="checkbox"/> Data sharing agreement
<input type="checkbox"/> Data sharing and processing agreement (DSPA)
<input checked="" type="checkbox"/> Audit
<input checked="" type="checkbox"/> Staff training
<input type="checkbox"/> Other

Section 5. HOW LONG ARE YOU KEEPING THE DATA AND WHAT WILL HAPPEN TO IT AFTER THAT TIME?

17. How long are you planning to use the data for?

Vital sign and observation records are an element of the respective EPR system and will be archived or preserved as per the retention period of the EPR system data.

18. How long do you intend to keep the data?



Essex Partnership University NHS Foundation Trust

Recorded data intended for permanent patient records and stored in the respective EPR system or output from the Oxevision system including Oxevision Observation systems is saved in perpetuity.

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, Patient Health Record Data, or any other personally identifiable information which can be linked to this data (the “Non-Personal Data”).

Oxehealth only uses these data to provide the Oxehealth Service to the EPUT and for monitoring and improving the Oxehealth system.

Oxehealth has a retention policy of 2 years for these data, after which they will be deleted. They may be deleted sooner where requested by a Partner, at the end of the customer contract or when no longer required to support system performance.

Clear Video Data (CVD) is non-pixelated video footage that can be clipped and saved upon request if there is a situation that needs to be further investigated. The ward manager or nurse in charge (or their nominated deputies) and if out of hours, the on-call manager can request the clipping of the clear video data. The request must be made directly to Oxehealth within 24 hours of the situation or incident By calling the Oxehealth support line on 0800 030 6781. The requestor must provide their name, ward name, date and time of the CVD required, room number, and reason for the CVD request.

Upon receipt of a request, Oxehealth will clip and save CVD. Oxehealth will then seek authorisation from the named CVD approvers. Once authorisation has been granted, Oxehealth attend the site to transfer the clipped CVD to a secure USB for delivery to The Lodge. An access PIN for the USB will be emailed to the Trust’s designated recipient. The USB will be secured with the legal team for review and assessment. CVD must always be under the control of the legal department. Clear video data will not be released directly to the ward and are managed via protocols governing the use of the data. (Please contact the Legal team/DPO for further guidance). To ensure immediate action and lessons are identified the Associate Director for the service and the Head of Patient Safety Incident Team will be authorised to access the clear video data. Any other requests will need to be discussed with the Legal team / DPO. Clear video data is automatically deleted from the local Oxevision server (on EPUT sites) after 24 hours.



Essex Partnership University

NHS Foundation Trust

Source: Standard Operating Procedure for the use of the Oxehealth Oxevision (Vision Based Patient Monitoring technology)
In EPUT Inpatient bedrooms, seclusion rooms and HBPOS facilities version 9.1, 14/11/2023

19. What will happen to the data at the end of this period?

Put an [x] next to all that apply.

<input checked="" type="checkbox"/> Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction)
<input type="checkbox"/> Permanent preservation by transferring the data to a Place of Deposit run by the National Archives
<input type="checkbox"/> Transfer to another organisation
<input type="checkbox"/> Extension to retention period – with approved justification
<input type="checkbox"/> It will be anonymised and kept
<input type="checkbox"/> The Controller(s) will manage as it is held by them
<input type="checkbox"/> Other

Section 6. HOW ARE PEOPLE'S RIGHTS AND CHOICES BEING MET?

20. How will you comply with the following individual rights (where they apply)?

Individual right	How you will comply (or state <i>not applicable</i> if the right does not apply)
The right to be informed The right to be informed about the collection and use of personal data.	We have assessed how we should inform individuals about the use of data for Oxehealth. Put an [x] next to all that apply.



	<input checked="" type="checkbox"/>	Privacy notice(s) for all relevant organisations
	<input checked="" type="checkbox"/>	Information leaflets
	<input checked="" type="checkbox"/>	Posters
	<input checked="" type="checkbox"/>	Letters
	<input checked="" type="checkbox"/>	Emails
	<input type="checkbox"/>	Texts
	<input type="checkbox"/>	Social media campaign
	<input checked="" type="checkbox"/>	DPIA published (best practice rather than requirement)
	<input checked="" type="checkbox"/>	Other – Care plans and My Care My Recovery
	<input type="checkbox"/>	Not applicable



Essex Partnership University

NHS Foundation Trust

<p>The right of access The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.</p>	Right to access follows the same guidance as other SARS access requests.
<p>The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete.</p>	Access to records will help with this. Each request will be considered on a case by case basis.
<p>The right to erasure The right to have personal data erased, if applicable.</p>	Legally obliged to maintain permanent records.
<p>The right to restrict processing The right to limit how their data is used, if applicable.</p>	Each request will be considered on a case by case basis.
<p>The right to data portability The right to obtain and re-use their personal data, if applicable.</p>	N/A
<p>The right to object The right to object to the use and sharing of personal data, if applicable.</p>	Each request will be considered on a case by case basis.



21. Will the national data opt-out need to be applied?

Put an [x] next to the one that applies.

<input type="checkbox"/> Yes
<input checked="" type="checkbox"/> No
<input type="checkbox"/> Unsure

22. Will any decisions be made in a purely automated way without any human involvement (automated decision making)?

Put an [x] next to the one that applies.

<input type="checkbox"/> Yes - go to question 22a
<input checked="" type="checkbox"/> No - skip to question 23
<input type="checkbox"/> Unsure - add as a risk with an action to find out

a. Where the effect of the automated decision on the individual is substantial, how will you uphold an individual's right not to be subjected to a decision solely made by automated means)?

b. Are you using any special category data as part of automated decision making?

<input type="checkbox"/> Yes
<input type="checkbox"/> No

23. Detail any stakeholder consultation that has taken place (if applicable).



Essex Partnership University

NHS Foundation Trust

An existing DPIA is in place. There is an assumption that this stakeholder consultation has already occurred in previous DPIA versions.

Section 5 of the Oxevision SOP v9.1 outlines the communication requirements for patients and carers as well as the implicit consent approach applied by the Trust.

<https://input.eput.nhs.uk/TeamCentre/cs/Oxe/TeamDocuments/SOP%20Oxevision%20v9.1.pdf>

Section 7. WHICH ORGANISATIONS ARE INVOLVED?

24. List the organisation(s) that will decide why and how the data is being used and shared (controllers).

Data ownership is laid out in the Oxehealth Services Agreement.

The Partner owns all right, title and interest in the Clear Video Data, Patient Health Record Data, Staff Identification Data, Anonymised (blurred) Video Data and User Interface Output Data.

Oxehealth owns all right, title and interest in the Algorithm Processed Data and Empty Room Video Data. For the avoidance of doubt, Algorithm Processed Data and Empty Room Video Data constitutes Oxehealth Confidential Material.

25. List the organisation(s) that are being instructed to use or share the data (processors).

Oxehealth

26. List any organisations that have been subcontracted by your processor to handle data

N/A

27. Explain the relationship between the organisations set out in questions 24, 25 and 26 and what activities they do



Essex Partnership University

NHS Foundation Trust

The current scope of work is to convert OxeObs (Oxehealth) data for inclusion into Mobius or Paris (EPUT). For Mobius, that includes an OCR export from the OxeObs PDF export to Mobius via Laserfiche. Paris remains in a manual upload state. The end state may not include a conversion for Paris but a direct upload of the PDF export to Paris via Paris Connect. The project board and team are exploring options to ensure sustainability and quality.

28. What due diligence measures and checks have been carried out on any processors used?

Put an [x] next to all that apply.

<input checked="" type="checkbox"/> Data Security and Protection Toolkit (DSPT) compliance
<input checked="" type="checkbox"/> Registered with the Information Commissioner's Office (ICO) - ZA065748 - Reg expires August 2024
<input checked="" type="checkbox"/> Digital Technology Assessment Criteria (DTAC) assessment
<input checked="" type="checkbox"/> Stated accreditations MD 633238 The Oxehealth Vital Signs software is a class IIa medical device in the UK and EU. Vital Signs Basic UDI-DI for identification in Eudamed: 506075145VITALSIGNSSFF. https://www.oxehealth.com/medical-device-disclaimer
<input checked="" type="checkbox"/> Cyber Essentials or any other cyber security certification - Cyber Essentials Plus 7bffcd5f-01af-4c81-ac2a-7b10a20860d3
<input type="checkbox"/> Other checks

Section 8. WHAT DATA PROTECTION RISKS ARE THERE AND WHAT MITIGATIONS WILL YOU PUT IN PLACE?

29. Complete the risk assessment table. Use the *risk scoring table to decide on the risk score.

Risk assessment table



Essex Partnership University

NHS Foundation Trust

Risk ref no.	Description	Risk score* (L x I)	Mitigations	Risk score* with mitigations applied
01	Power outage affecting Trust servers leading to loss of availability of data	10	Backup generators kick in if main system fails	2
02	Information is stored in unrestricted network areas leading to inappropriate access to data	8	Ensure project team have dedicated network space with access restricted to team members	2
03	Data is not up to date	12	The controller will send out daily notifications of updates	4
04	Oxehealth system not working	12	Oxehealth will make sure they are on top of things but if not then we have a backup and observations and vitals are done on paper form	2

***Risk scoring table**

		Impact (I)				
		Negligible (1)	Low (2)	Moderate (3)	Significant (4)	Catastrophic (5)
Likelihood (L)	Rare (1)	1	2	3	4	5
	Unlikely (2)	2	4	6	8	10
	Possible (3)	3	6	9	12	15

Likely (4)	4	8	12	16	20
Almost certain (5)	5	10	15	20	25

30. Detail any actions needed to mitigate any risks, who has approved the action, who owns the action, when it is due and whether it is complete.

Risk ref no.	Action needed	Action approver	Action owner	Due date	Status e.g. outstanding/ complete
01	Backup generators kick in if main system fails	EPUT	EPUT	Ongoing	Ongoing
02	Ensure project team have dedicated network space with access restricted to team members	EPUT	EPUT	Ongoing	Ongoing
03	Controller will send out daily notifications of updates	OxeHealth	OxeHealth	Ongoing	Ongoing
04	Oxehealth will make sure they are on top of things but if not then we have a back up and observations and vitals are done paper form	OxeHealth	OxeHealth	Ongoing	Ongoing

Section 9. REVIEW AND SIGN OFF



Essex Partnership University

NHS Foundation Trust

Individual completing DPIA	Name:	[REDACTED]
	Job Title:	Oxevision System Manager (Interim)
	Form completion date:	10 May 2024
Information Governance	Name:	[REDACTED]
	Job Title:	Information Governance Manager
	Signature:	
	Form approval date:	14.05.24
Senior Information Risk Officer	Name:	[REDACTED]
	Job Title:	Executive Director of Strategy, Transformation and Digital
	Signature:	
	Form approval date:	15.05.24
Data Protection Officer	Name:	[REDACTED]
	Job Title:	Deputy Data Protection officer
	Signature:	
	Form approval date:	14.05.24
Other approvals	Name:	
	Job Title:	
	Signature:	
	Form approval date:	
Other approvals	Name:	
	Job Title:	



Essex Partnership University

NHS Foundation Trust

	Signature:	
	Form approval date:	

Annex

The laws that health and care organisations rely on when using your information

Data protection laws mean that organisations must identify which law they are relying on when sharing information. For example if an organisation is sharing information, because they are required by law to do so, they need to identify which law is requiring this. The following are the most likely laws that apply when using and sharing information in health and care. This list is not exhaustive.

Abortion Act 1967 and Abortion Regulations 1991

Requires that health and care staff share information with the Chief Medical Officer about abortion treatment they have provided.

Access to Health Records Act 1990

Allows access the health records of deceased people, for example to personal representatives or those who have a claim following the deceased person's death.

Care Act 2014

Defines how NHS organisations and local authorities must provide care and support to individuals, including for the management of safeguarding issues. This includes using information to assess any person who appears to require care and support.

Children Act 1989

Sets out the duties of local authorities and voluntary organisations in relation to the protection and care of children. It requires organisations that come into contact with children to cooperate and share information to safeguard children at risk of significant harm.



Control of Patient Information Regulations 2002 (COPI)

Allows information to be shared for specific reasons in relation to health and care, such as for the detection and prevention of cancer, to manage infectious diseases, such as measles or COVID-19. It also allows for information to be shared where support has been given for research or by the Secretary of State for Health and Social Care.

Coroners and Justice Act 2009

Sets out that health and care organisations must pass on information to coroners in England.

Employment Rights Act 1996

Sets out requirements for employers in relation to their employees. This includes keeping records of staff when working for them.

Equality Act 2010

Protects people from discrimination based on their age, disability, gender reassignment, pregnancy or maternity, race, religion or belief, sex, sexual orientation. Organisations may need to use this information to ensure that they are complying with their responsibilities under this Act.

Female Genital Mutilation Act 2003

Requires health and care professionals to report known cases of female genital mutilation to the police.

Fraud Act 2006

Defines fraudulent activities and how information may be shared, for example with the police, to prevent and detect fraud.

Health and Social Care Act 2008 and 2012

Sets out the structure of the health and social care system and describes the roles of different types of organisations. It sets out what they can and can't do and how they can or can't use information. It includes a duty for health and care staff to share information for individual care, unless health and care organisations have a reasonable belief that you would object. In addition, health and care organisations may need to provide information to:

- The Secretary of State for Health and Social Care
- NHS England, which leads the NHS in England and provides information, data and IT systems for health and social care



- The Care Quality Commission, which inspects health and care services
- The National Institute for Health and Care Excellence (NICE), which provides national guidance and advice to improve health and care

Health and Social Care (Community Health and Standards) Act 2003

Allows those responsible for planning health and care services to investigate complaints about health and care organisations they have a contract with.

Health Protection (Notification) Regulations 2010

Requires health professionals to help manage the outbreaks of infection by reporting certain contagious diseases to local authorities and to the UK Health Security Agency. The UK Health Security Agency is responsible for protecting people from the impact of infectious diseases.

Human Fertilisation and Embryology Act 1990

Requires health organisations to report information about assisted reproduction and fertility treatments to the Human Fertilisation and Embryology Authority.

Human Tissue Act 2004

Requires health organisations to report information about transplants, including adverse reactions to the Human Tissue Authority.

Inquiries Act 2005

Sets out requirements in relation to public inquiries, such as the UK COVID-19 Inquiry. Public inquiries can request information from organisations to help them to complete their inquiry.

Local Government Act 1972

Sets out the responsibilities of local authorities in relation to social care including managing care records appropriately. For example, it lays out how they should be created, stored and how long they should be kept for.



NHS Act 2006

Sets out what NHS organisations can and can't do and how they can or can't use information. It allows confidential patient information to be used in specific circumstances for purposes beyond individual care. These include a limited number of approved research and planning purposes (see Control of Patient Information Regulations 2002 (COPI) above). Information can only be used where it is not possible to use information which doesn't identify you, or where seeking your explicit consent to use the information is not practical. The Act also sets out that information must be shared for the prevention and detection of fraud in the NHS.

Public Records Act 1958

Defines all records created by the NHS or local authorities as public records. This includes where organisations create records on behalf of the NHS or local authorities. These records therefore need to be kept for certain periods of time, including permanently in some cases.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

Requires employers to report deaths, major injuries and accidents to the Health and Safety Executive, the national regulator for workplace health and safety.

Safeguarding Vulnerable Groups Act 2006

Sets out requirements for organisations who work with vulnerable to share information and to perform pre-employment checks with the Disclosure and Barring Service (DBS), which is responsible for helping employers make safer recruitment decisions.

Statistics and Registration Service Act 2007

Allows health organisations that plan services and local authorities to receive and disclose health and care information to the Office for National Statistics (ONS). The ONS is the UK's largest independent producer of official statistics.

Terrorism Act 2000 and Terrorism Prevention and Investigation Measures Act 2011

Requires any person to share information with the police for the prevention and detection of terrorism related crimes.



Essex Partnership University
NHS Foundation Trust

The Road Traffic Act 1988

Requires any person to provide information to the police when requested to help identify a driver alleged to have committed a traffic offence.

Confidential



Oxehealth

Data Protection Impact Assessment

Essex Partnership University NHS Foundation Trust

August 2023

Note to Partner: As part of its commitment to good data protection governance, Oxehealth provides this DPIA template to assist its Partners with their obligations under Article 35 of the GDPR. The processing of data by Essex Partnership University NHS Foundation Trust staff is not in the scope of this DPIA, the purpose of which is to outline processing activities of Oxehealth as a data processor on behalf of Essex Partnership University NHS Foundation Trust when providing the Oxevision service. It remains the Partner's sole responsibility to conduct a DPIA that meets the requirements of applicable law. Nothing in this DPIA template constitutes legal advice.

Contents

1. Introduction	3
2. Identification of the need for a DPIA	3
3. Information Flows.....	6
A. Types of Data	6
B. The Data Journey	9
C. Usage of Data at Oxehealth	12
D. Storage and Retention	13
E. Data Ownership	15
F. Data Security.....	15
G. Oxehealth Standards, Certifications and Registrations	16
H. NHS Application and Data Standards	16
4. Privacy and Related Risks	17
5. Proposed Privacy Solutions	18
6. DPIA Outcomes.....	22
Appendix 1	23
Appendix 2	24

1. Introduction

Oxehealth is a spin-out from Oxford University which develops proprietary software that supports clinical staff in caring for the safety and health of their patients.

Essex Partnership University NHS Foundation Trust provides community health, mental health and learning disability services for a population of approximately 1.3 million people throughout Bedfordshire, Essex, Suffolk and Luton.

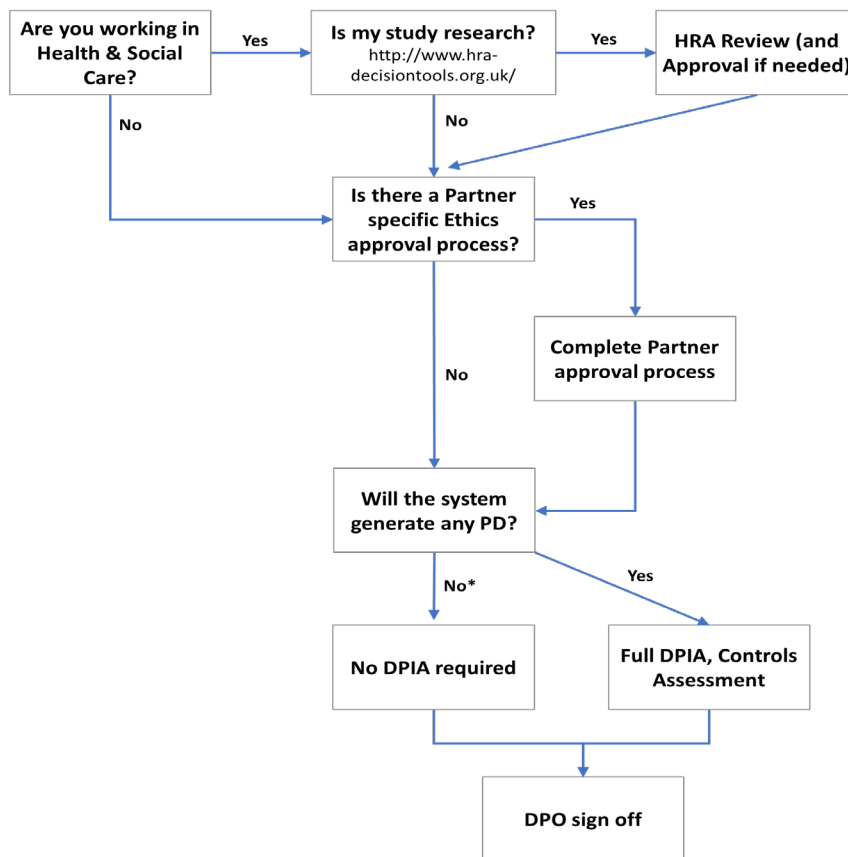
In this project, Essex Partnership University NHS Foundation Trust wishes to deploy the Oxehealth Software & Oxehealth Services to improve and supplement its patient care and safety monitoring regimes.

The service agreement with Essex Partnership University NHS Foundation Trust includes the following Oxehealth software modules:

- Oxevision Observations

2. Identification of the need for a DPIA

Before commencing any project with a Partner, Oxehealth performs a review of its Compliance Protocol, a simple and specific workflow that steps through the potential questions and decision points relating to the compliance and approval steps needed prior to commencing work with a Partner:



*Note – a DPIA is always completed by Oxehealth in either scenario

In the case of Essex Partnership University NHS Foundation Trust, the Protocol responses are:

Question	Response	Action Needed
Are you working on Health & Social Care?	Yes	-
Is my study research?	No	-
Are any subjects patients?	Yes	Data Protection Officer sign off needed
Is there a local, specific approval process	No	-
Will the system generate any Personal Data?	Yes	Full DPIA and Controls Assessment needed
Are there any Essex Partnership University NHS Foundation Trust specific Data Holding requirements?	No	-

Identifying 'high risk' processing under the GDPR and UK Data Protection Act

A DPIA must be carried out whenever processing of personal data is likely to result in a high risk to individuals. The Information Commissioner's Office (ICO) has identified a list of activities it considers to be 'high risk', which sit alongside the risk triggers in the GDPR and those identified by the European Data Protection Board (EDPB). Of these high risk criteria, Oxehealth's software may involve:

- **The use of innovative technology (ICO risk trigger):** Oxehealth's software is a novel technology not previously deployed by **Essex Partnership University NHS Foundation Trust**.
- **Systematic monitoring (EDPB risk trigger):** Whilst CCTV is used throughout Essex Partnership University NHS Foundation Trust facilities and in seclusion rooms, it is not currently used in the patient bedrooms proposed to be used for the project. In this project, raw video data recorded by digital video cameras in patient rooms will be processed by the software to deliver the alerts which appear on display units to help **Essex Partnership University NHS Foundation Trust** improve its current patient safety and activity monitoring regimes. While clinicians will not be able to use the video feed as CCTV they will be required to view 15 seconds of raw video when taking vital signs measurements to ensure they are taken accurately.
- **Sensitive data or data of a highly personal nature (EDPB risk trigger):** The system captures health data (including vital signs and other patient healthcare data alongside patient name and patient identification number) regarding patients under the care of **Essex Partnership University NHS Foundation Trust**.
- **Data concerning vulnerable data subjects (EDPB risk trigger):** The data subjects are patients at **Essex Partnership University NHS Foundation Trust**, and as such potentially vulnerable.

The output of Oxehealth's Compliance Protocol and the identification of four potential high risk criteria clearly indicates the need for a DPIA to be undertaken.

3. Information Flows

A. Types of Data


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”.

Data is also collected and stored on the “local secure server” via an optional connection to an Electronic Patient Record (EPR) and/or users entering data directly.

Finally, some of the data collected is stored on secure remote servers based in the UK provided by Oxehealth’s cloud storage provider Amazon Web Services (AWS) - these are referred to as “cloud servers”.

In this project, the data falls into one of the following possible categories:

Non-Personal Data

- a) Anonymised (blurred) Video Data (AVD) - Oxehealth will anonymise the camera feed so that the individual is not identifiable from the video. Some modules within the Oxehealth Software permit staff 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) Algorithm Processed Data (APD)- 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) User Interface Output Data (UIOD) - When the algorithm has completed its processing of the 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 that was taken) which are supplied to an output server (known as the User Module) so that they can be displayed to Essex Partnership University NHS Foundation Trust’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.

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 (see section C” usage of data at Oxehealth”, 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 above). Clear Video Data will be selectively collected in short episodes for specific purposes, so the total volume of video will be relatively low. See “D. Storage and Retention” for further details.

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. See “C. Usage of Data at Oxehealth” below for usage of Clear Video Data.

Clear Video Data is held separately to the Anonymised (blurred) Video Data, Algorithm Processed Data and User Interface Output Data.

- b) Patient Health Record Data (PHRD) - The Oxevision Observations product module provides the ability to assign patients to bedrooms and to gather patient observations of vital signs (using the Vital Signs product module described above) and other patient observations made. Patient identifying data will be provided by Essex Partnership University NHS Foundation Trust via either a secure connection to the Essex Partnership University NHS Foundation Trust EPR system, or by Partner staff entering this data, and will include patient name and their uniquely identifying number (e.g. NHS number, or other unique identifier for the patient or patient episode). Further health record data will be generated by the Oxevision Observations product module during the course of patient observations, including their vital signs, other patient observation data such as location and presentation, observation level or protocol and other risk assessment information. All Patient Health Record Data is personal data.

Patient Health Record Data is required in order to provide Essex Partnership University NHS Foundation Trust staff with the observation data required to manage and care for their patients. The data is encrypted and held on the local secure server within the user interface software. Patient Health Record Data is also included in Observation reports which are emailed from the system to Essex Partnership University NHS Foundation Trust staff (via Egress) when requested by Essex Partnership University NHS Foundation Trust staff.

Further Oxehealth processing of the data is limited to backup of the encrypted user interface data to its secure AWS cloud servers, which is required to provide service continuity and restoration of Patient Health Record Data in the event of hardware failures and other disaster scenarios.

Patient Health Record Data may also be transferred back to Essex Partnership University NHS Foundation Trust over a secure API connection to the Essex Partnership University NHS Foundation Trust EPR.

c) Staff Identification Data (SID)

The email address of an appointed Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust. Email addresses of all Essex Partnership University NHS Foundation Trust staff who request a report are also recorded in this way. This data is stored on the local secure server at Essex Partnership University NHS Foundation Trust, and in Oxehealth's secure cloud services: Gitlab as part of site configuration and in AWS and/or Egress for emailing the reports.

As part of user identification in the Oxevision Observations product module, credentials (staff name and/or email address) to identify the Essex Partnership University NHS Foundation Trust staff operating the software are processed and stored by the local secure server. In addition agency name is processed where the staff member taking the observations is temporary staff.

Staff identification data are required to access the Oxevision Observations product module functions that modify Patient Health Record Data to enable Essex Partnership University NHS Foundation Trust to ensure the correct observations are assigned to the staff performing them for audit reasons. Staff identifiers are stored and used in the local secure server software to provide an immutable audit trail to Essex Partnership University NHS Foundation Trust of those Essex Partnership University NHS Foundation Trust staff adding and modifying Patient Health Record Data. These identifiers are also included in Observation reports which are emailed from the system to Essex Partnership University NHS Foundation Trust staff. Further Oxehealth processing of the data is limited to backup of the encrypted data to its secure AWS cloud servers, which is required to provide service continuity and restoration of Staff Identification Data alongside the Patient Health Record Data in the event of hardware failures and other disaster scenarios.

- d) Anonymised (blurred) Video Data, Algorithm Processed Data, and User Interface Output Data – described above are usually classed as non-personal data. However, where the Oxevision Observations product module is in use, these are all personal data for the period of time where there is Patient Health Record Data linked to them, which would enable the individual to whom this data relates to be identified. While this data is classed as Personal Data (until the Patient Health Record to which it relates has been deleted from the local secure server and backups), it is tagged as Personal Data when stored on Oxehealth's secure cloud servers and is used for limited purposes only as outlined in "Section C: Usage of Data at Oxehealth".

B. The Data Journey

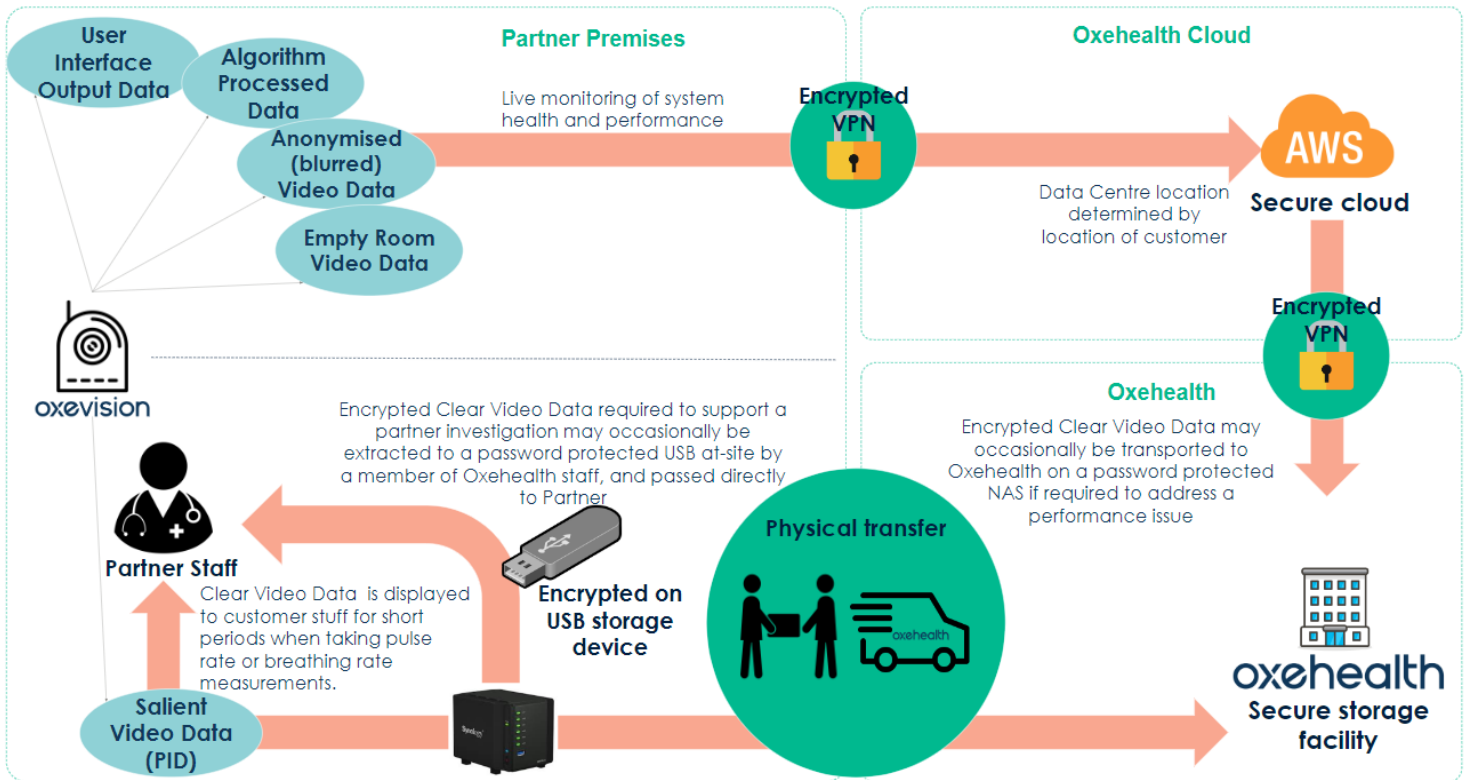


Figure 1. Data Flows from the Oxevision software on Partner Premises to Oxehealth

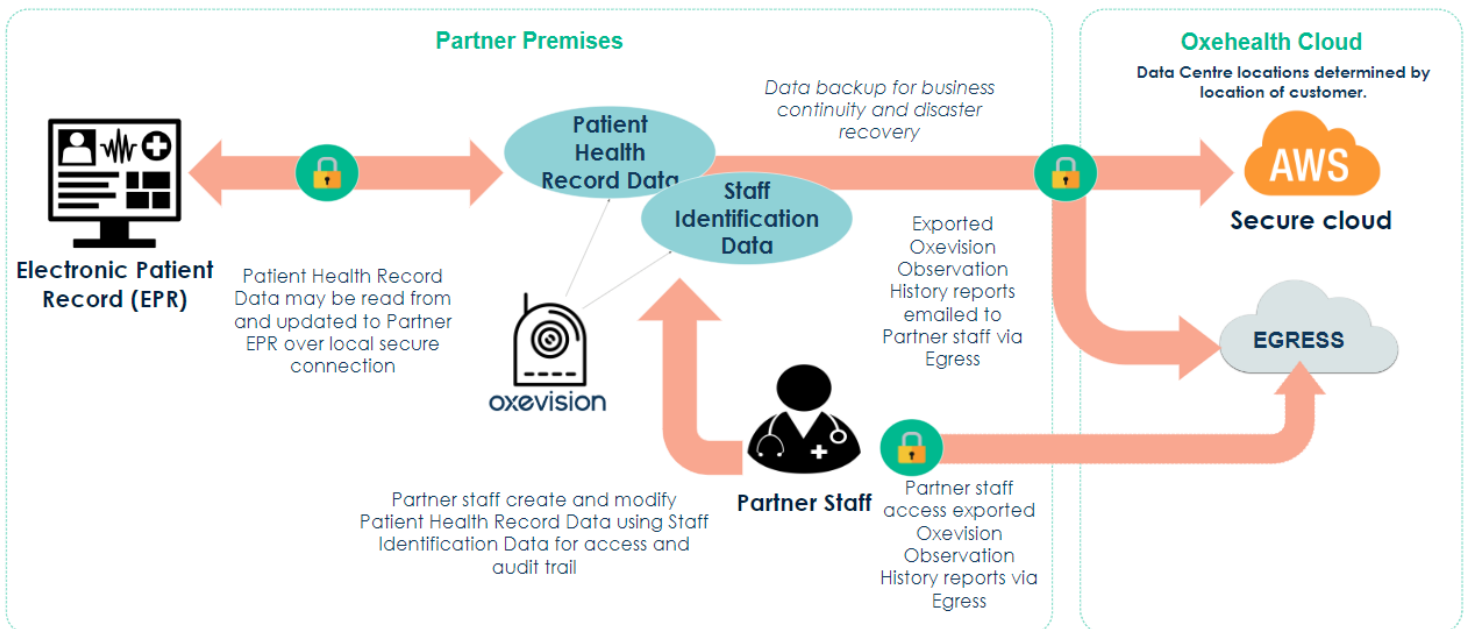


Figure 2. Data Flows from the Partner Electronic Patient Record (EPR) and the Oxevision Observations software on Partner Premises to Oxehealth

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 the secure Essex Partnership University NHS Foundation Trust facility.

The Oxehealth Software modules hosted on the local secure server are accessed by Essex Partnership University NHS Foundation Trust staff through fixed monitors located securely on Essex Partnership University NHS Foundation Trust'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. Essex Partnership University NHS Foundation Trust staff interact with various data types including Clear Video Data in their day-to-day use of the system.

The processing of this data by Essex Partnership University NHS Foundation Trust staff is not in the scope of this DPIA, the purpose of which is to outline processing activities of Oxehealth as a data processor on behalf of Essex Partnership University NHS Foundation Trust when providing the Oxevision service.

Patient Health Record Data is collected on the local secure server through two means:

1. Via secured, encrypted connection to the Essex Partnership University NHS Foundation Trust EPR over Ethernet cabling connecting the Oxehealth system to the Essex Partnership University NHS Foundation Trust infrastructure; and/or
2. Through staff interaction with the Oxehealth software modules through connections as described above.

From the local secure server, data travels to Oxehealth via two mediums - over the internet and by the physical movement of storage devices by Oxehealth staff.

a) Data that travels to Oxehealth via the Internet (over encrypted connection)

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 Essex Partnership University NHS Foundation Trust as per the defined Service Level Agreements (SLAs) in the Oxehealth Service Agreement.

Oxehealth will routinely transport encrypted Personal Data via the internet in the form of backups of local secure server software internal state, including Patient Health Record Data and Staff Identification Data. This does not include Clear Video Data. These data are backed up to Oxehealth's secure AWS cloud servers to provide a data recovery backup of the Oxevision Observations product module.

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 AWS cloud servers, and from the secure AWS cloud servers to secure Oxehealth facilities.

Personal data (the Patient Health Record Data and Staff Identification Data) is additionally encrypted prior to storage, giving two levels of unique encryption protection while being transferred.

b) Data that arrives at Oxehealth via the physical movement of storage devices

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 (See “C. Usage of Data at Oxehealth” below for usage of Clear Video Data), 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 Essex Partnership University NHS Foundation Trust via three mediums - over an API connection to Essex Partnership University NHS Foundation Trust IT infrastructure, over the internet via secure connection to Egress, and by the physical movement of storage devices by Oxehealth staff.

a) Data that is transferred via the physical movement of storage devices

If Clear Video Data has been extracted to support a Essex Partnership University NHS Foundation Trust investigation (i.e. purpose (2) in “C. Usage of Data at Oxehealth”), the Clear Video Data clip will be delivered by a member of Oxehealth staff extracting the Clear Video Data clip directly from the local secure server on Essex Partnership University NHS Foundation Trust premises onto an encrypted USB stick and passing it directly to the appropriate member of Essex Partnership University NHS Foundation Trust staff.

b) Data that is transferred via a local connection to the Electronic Patient Record (EPR)

Oxehealth will transfer Patient Health Record Data where required to the EPR over a local, secure, encrypted connection to an approved endpoint under the control of IT.

This data is transferred to provide with permanent health record data as collected from the Oxevision Observations product module.

c) Data that is transferred via the internet to Partner staff via secure connection to Egress

Oxevision Observation History reports containing Patient Health Record Data and Staff Identification Data will be generated by Essex Partnership University NHS Foundation Trust staff using the Oxevision Observations Module. These reports can be exported to Essex Partnership University NHS Foundation Trust staff via email. The email and attachments will be transferred through a secure SSL connection to Egress (UK platform) via Oxehealth’s Microsoft Exchange Server (located in the UK) and a notification will be emailed to Essex Partnership University NHS Foundation Trust staff. Essex Partnership University NHS Foundation Trust staff will be required to authenticate to the Egress platform in order to view the encrypted email attachments.

C. Usage of Data at Oxehealth

Non-Personal Data

- a) 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, Patient Health Record Data, or any other personally identifiable information which can be linked to this data (the “Non-Personal Data”).

Oxehealth only uses these data for the purpose of providing the Oxehealth Service to the Essex Partnership University NHS Foundation Trust and for the purpose of monitoring and improving the Oxehealth system.

Oxehealth has a retention policy of 2 years for these data, after which they will be deleted. They may be deleted sooner where requested by a Partner, at the end of the customer contract or when no longer required to support system performance.

- b) Empty Room Video Data does not constitute personal data under any circumstances, and is used by Oxehealth for the purpose of monitoring and improving the Oxehealth system. This data is used by the algorithm and may be kept for the lifetime of the system.

Personal Data

a) Clear Video Data

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 Essex Partnership University NHS Foundation Trust identifies a performance issue with Oxevision, or is alerted to a potential performance issue by Oxehealth staff, and the issue cannot be otherwise resolved, Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust Personnel 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 staff with access to the data will 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 UK staff are DBS screened. No Clear Video Data will be used for research, marketing, or publicity purposes.

b) Patient Health Record Data and Staff Identification Data

1. Patient Health Record Data is processed and stored on the local secure server to provide the Oxevision Observations product module to Essex Partnership University NHS Foundation Trust staff.

Oxehealth staff will have access to this data only in its encrypted format and will not decrypt the data or view any decrypted rendition of the data during any of the remote monitoring and maintenance that Oxehealth routinely performs.

2. Staff Identification Data is processed on the local secure server to provide user access to Patient Health Record Data. The data is also processed and stored to provide an audit log of user creation and modification of Patient Health Record Data.

Oxehealth staff will have access to this data only when required to provide technical support or restore the Oxevision Observations service. The data will normally be encrypted but on very rare occasions, and only with Essex Partnership University NHS Foundation Trust consent, Oxehealth staff may need to decrypt the data.

3. Oxehealth will store a backup of Patient Health Record Data and Staff Identification Data on the secure AWS cloud servers to provide service continuity and recovery from disaster scenarios for the Oxevision Observations product module.

Oxehealth staff will have access to this data only where required to provide technical support or restore the Oxevision Observations service. The data will normally be encrypted but on very rare occasions, and only with Essex Partnership University NHS Foundation Trust consent, Oxehealth staff may need to decrypt the data.

4. Where otherwise anonymised data (Anonymised (blurred) Video Data, Algorithm Processed Data, and User Interface Output Data) are linked to a Patient Health Record and therefore classed as personal data, this data is tagged as Personal Data where it is stored in Oxehealth's secure cloud and Oxehealth are alerted via warnings displayed in tooling if they try to access this data.

While this data is classified as personal data, Oxehealth will use it only to monitor the performance of the software and provide support to customers, to resolve issues with the Oxevision service for the specific room the data is associated with. When the data no longer has Patient Health Record data associated with it and it is classified as anonymised data it will be used for the purposes outlined in the 'non personal data' section above.

D. Storage and Retention

Non-Personal Data

- 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 these data, after which they will be deleted. They may be deleted sooner when requested by a Partner, at the end of the customer 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 Essex Partnership University NHS Foundation Trust 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 customer contract, or when no longer needed to support system performance.

Personal Data

a) Clear Video Data

The Clear Video Data is stored on the local secure server for [24hrs] after which it is deleted. 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 Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust, to enable the delivery of the Oxehealth Service to Essex Partnership University NHS Foundation Trust to the contracted SLA, to ensure that the Oxehealth system is continuously optimised for all Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust. Oxehealth will retain this data until the end of the contract with Essex Partnership University NHS Foundation Trust, until it is no longer needed, or until Essex Partnership University NHS Foundation Trust instructs Oxehealth to delete it, whichever is earlier.

Data collected for serious incident review is not retained by Oxehealth, but provided directly to the Essex Partnership University NHS Foundation Trust to support their investigation.

Twice per year, Oxehealth provides Essex Partnership University NHS Foundation Trust with a Video Data Report which details the volume, retention period and retention purpose for any Clear Video Data collected for Essex Partnership University NHS Foundation Trust for the purposes outlined in "C. Usage of Data at Oxehealth". 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 Essex Partnership University NHS Foundation Trust, 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) Patient Health Record Data and Staff Identification Data

Staff Identification data stored on the local secure server and on cloud-servers (AWS and Gitlab) for the purpose of providing reports to Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust

Except where associated with a Patient Health Record, Staff Identification Data generated as part of the Oxevision Observations module is stored by the local secure server software usually for 30 days (although Oxehealth can provide a different retention period if desired), after which time, the data is removed from the database by the software

Patient Health Record Data and Staff Identification Data associated with the Patient Health Record is stored by the local secure server software until 28 days after the patient leave date (although Oxehealth can provide a different retention period if desired), after which time, the data is removed from the database by the software.

Patient Health Record Data and Staff Identification Data referred to above is backed up to Oxehealth's secure AWS cloud servers where it is retained as a data backup for a further 30 days and is then securely deleted from storage.

Where Patient Health Record Data and Staff Identification Data is stored on the secure Egress server as part of an exported Oxevision Observations History report, Partners can delete the reports once they have successfully downloaded them to their local storage. Oxehealth can additionally configure a retention period on Egress at customer request.

Anonymised (blurred) Video Data, Algorithm Processed Data and User Interface Output data is classed as personal data only while there is Patient Health Record data associated with it, after which it becomes non-personal data. The retention period of this data as Personal data therefore matches the retention period of the associated Patient Health Record data outlined above, after which the retention period for non-personal data applies.

E. Data Ownership

Data ownership is laid out in the Oxehealth Services Agreement.

The Partner owns all right, title and interest in the Clear Video Data, Patient Health Record Data, Staff Identification Data, Anonymised (blurred) Video Data and User Interface Output Data.

Oxehealth owns all right, title and interest in the Algorithm Processed Data and Empty Room Video Data. For the avoidance of doubt, Algorithm Processed Data and Empty Room Video Data constitutes Oxehealth Confidential Material.

F. Data Security

Data Generated by the Oxevision system will be stored on the local compute equipment securely at Essex Partnership University NHS Foundation Trust while it is being recorded. (local secure server and network attached storage). In these storage locations, Personally Identifiable Data (Clear Video Data, Staff identification Data and Patient Health Record Data) will be encrypted at rest to the AES 256 standard.

All data transmission between local compute equipment at Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust site, uses a unique set of credentials for Virtual Private Network (VPN), remote machine access and fileserver 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-hr security guards.

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 Essex Partnership University NHS Foundation Trust 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.

G. Oxehealth Standards, Certifications and Registrations

Oxehealth is ISO/IEC 13485, ISO/IEC 27001 and Cyber Essentials Plus certified 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

H. NHS Application and Data Standards

Oxehealth complies with the DCB0129 clinical risk management standard and has completed the DAPB0086 Data Security & Protection Toolkit (DSPT) with "standards exceeded".

4. Privacy and Related Risks

An assessment of the proposed project identified the following potential risks in relation to the privacy of an individual:

Risk ID	Privacy Issue	Compliance Risk	Risk to the individual
1	Data disclosed inadvertently to a third party or data is lost.	GDPR Principle 6	The clear video data and/or patient health record 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.
2	Unnecessary intrusion into a patient's privacy	GDPR Principle 6	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	Identification of a patient by an Oxehealth staff member (i.e. if the patient is known personally to the staff member).	GDPR Principle 6	People external to Essex Partnership University NHS Foundation Trust 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.
4	Data retained longer than necessary	GDPR Principles 2 and 5	Data pertaining to a patient is retained longer than required, increasing the security risk and risk of a breach of confidentiality.
5	Patient unaware their data is being collected	GDPR Principles 1, 3 and 6	The patient is unaware of their rights under the General Data Protection Regulations (GDPR), and therefore unable to exercise them
6	Personal data is accidentally shared with Oxehealth	GDPR Principle 3	Personal data pertaining to a patient is processed by Oxehealth in systems not designed for personal data storage and processing, increasing the security risk and risk of a breach of confidentiality.
7	Data moved to another country with different data protection rules	GDPR Article 45	Reduced protection on rights and freedoms of data subjects.

8	Patient Health Record Data accuracy is compromised	GDPR Principle 4	Patient Health Record Data may be entered inaccurately, or amended by Essex Partnership University NHS Foundation Trust staff, leading to reduced quality of care and potentially harm.
---	--	------------------	---

In addition to the risks to the individual, any non-compliance could lead to regulatory action, reputational damage, or loss of public trust in Essex Partnership University NHS Foundation Trust.

5. Proposed Privacy Solutions

Following the identification of the potential risks in Section 4, a range of proposed solutions will be used to mitigate and control these risks. These are as follows:

Risk 1 – Data disclosed inadvertently to a third party or data is lost

The local secure server will be located at Essex Partnership University NHS Foundation Trust, and should be provided with appropriate physical and electronic access restricted to authorised Essex Partnership University NHS Foundation Trust or Oxehealth personnel by Essex Partnership University NHS Foundation Trust. In addition, the video data held on the local secure server is in a proprietary format which could not be viewed with publicly available software and all personal data is encrypted on the server to industry standard AES 256. The risk of data being disclosed or lost by a member of Essex Partnership University NHS Foundation Trust staff is therefore deemed to be very low.

To avoid a potential data leak due to theft or malicious electronic attack (and therefore mitigate the risk of accidental damage to or loss of data), Oxehealth have 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.
- Oxehealth has implemented access control and segregation of duties policies and employees the principle of least privilege to ensure granular access is granted to a limited subset of authorised Oxehealth employees only where required, is audited at planned intervals and is revoked when no longer needed.
- Portable storage devices are password or PIN protected and all personal data is encrypted to industry standard AES 256. When transported from customer site portal devices are always accompanied in transit by Oxehealth staff.
- All electronic communication of personal and non-personal data uses industry standard encrypted and authenticated protocols
- Oxehealth’s secure AWS cloud servers are ISO 27001 certified and they are externally audited for this certification as well as for SOC 2, and Oxehealth continue to monitor the security measures in place to ensure they are adequate. Staff Identification Data and Patient Health Record Data is encrypted to industry standard AES 256 on these servers.
- The Egress service used for securely transferring Oxevision Observation History Reports to Essex Partnership University NHS Foundation Trust staff is ISO 27001 certified and they are externally audited for this certification as well as for SOC 2. In addition they have been assessed as standards exceeded for the NHS standards exceeded. Oxehealth continue to monitor the security measures in place to ensure they are adequate. Staff Identification Data and Patient Health Record Data is encrypted to industry standard on Egress servers.

- When it is stored at Oxehealth facilities for the investigation of performance issues, Clear Video Data is stored on secure servers in a secure server room with limited keyholder access, in a building with door access control, CCTV and 24-hour security guards.
- 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 file servers are only accessible from the Oxehealth IP range, using individual logons only
- All data collected and generated by the Oxehealth system is anonymised as far as possible and personally identifiable data collection is kept to a minimum only where necessary to provide the service to the contracted standard.

Risk 2 – Unnecessary intrusion into a patient's privacy

As identified in Section 2 of 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 Essex Partnership University NHS Foundation Trust. 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.

The use of Clear Video Data is kept to a minimum, used only in accordance with the two purposes given in "C. Usage of Data at Oxehealth", all of which involve very short, isolated periods that occur: (1) on an occasional, non-routine basis to address performance issues under instruction from Essex Partnership University NHS Foundation Trust, or (2) to provide data to support Essex Partnership University NHS Foundation Trust with a serious incident review.

Risk 3 – Identification of a patient by an Oxehealth member of staff

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.

In the event of a member of the Oxehealth team being able to identify a patient involved in the project, Oxehealth will consult Essex Partnership University NHS Foundation Trust; the default action is to delete all data relating to that patient but Essex Partnership University NHS Foundation Trust; may instruct Oxehealth to pursue another course of action (for example, preserving the data for the purpose of an internal or external investigation).

Risk 4 – Data is retained longer than necessary

In the project, Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust (unless applicable law prevents Oxehealth from doing so).

Clear Video Data is stored on the local secure server at Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust staff or by engineers at Oxehealth on instruction from Essex Partnership University NHS Foundation Trust, 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.

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 Essex Partnership University NHS Foundation Trust with a Video Data Report which confirms the purpose, principles and review process for any Clear Video Data collected for the Partner and a log of the personal data retained, reasons for retentions and date of next review. The report will also include whether any Personally Identifiable 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 Essex Partnership University NHS Foundation Trust and will be deleted when Essex Partnership University NHS Foundation Trust 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 Essex Partnership University NHS Foundation Trust

Oxehealth will process all personal data generated in the project in accordance with this DPIA and documented instructions from Essex Partnership University NHS Foundation Trust, the Data Controller.

Except where associated with a Patient Health Record, Staff Identification Data is stored by the local secure server software usually for 30 days (although Oxehealth can provide a different retention period if desired), after which time, the data is removed from the database by the software

Patient Health Record Data and Staff Identification Data associated with a patient health record will be kept until 28 days after the patient leave date. In addition Essex Partnership University NHS Foundation Trust have the ability to request that Oxehealth delete Patient Health Record and Staff Identification data at any time.

Anonymised (blurred) Video Data, Algorithm Processed Data and User Interface Output Data is only personal data for as long as there is an associated Patient Health Record associated with them, after which they become non-personal data.

Risk 5 – Patient is unaware their data is being collected

Patients in the proposed rooms of Essex Partnership University NHS Foundation Trust are in the care of expert and highly trained Essex Partnership University NHS Foundation Trust staff who will take decisions in the best interest of those patients. Essex Partnership University NHS Foundation Trust will maintain a regime that informs patients in an appropriate fashion.

Risk 6 – Personal data is accidentally shared with Oxehealth

Patients in the proposed rooms of Essex Partnership University NHS Foundation Trust are in the care of expert and highly trained Essex Partnership University NHS Foundation Trust 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.

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

Risk 7 – Data is moved to another country with different data protection rules

All data generated by the Oxevision system is stored on local secure servers at Essex Partnership University NHS Foundation Trust site.

Some data (AVD, APD, UIOD, SID and PHRD) 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, a Sweden data centre for Swedish Partners, and a US data centre for US Partners.

Where Oxevision Observation Reports containing SID and PHRD are transferred to Essex Partnership University NHS Foundation Trust staff via Egress, the data is stored on Egress servers located in the UK for UK Partners, Sweden for Swedish Partners, and the US for US 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 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 Partners of these providers

Risk 8 – Patient Health Record Data accuracy is compromised

Patients in the proposed rooms of Essex Partnership University NHS Foundation Trust are in the care of expert and highly trained Essex Partnership University NHS Foundation Trust staff who will take decisions in the best interest of those patients. Essex Partnership University NHS Foundation Trust will maintain a regime that ensures accurate data collection and data processing.

Oxehealth will provide audit logging of user access to and modification of Patient Health Record Data to provide Essex Partnership University NHS Foundation Trust with the best possible audit and monitoring capability in maintaining accuracy of the data.

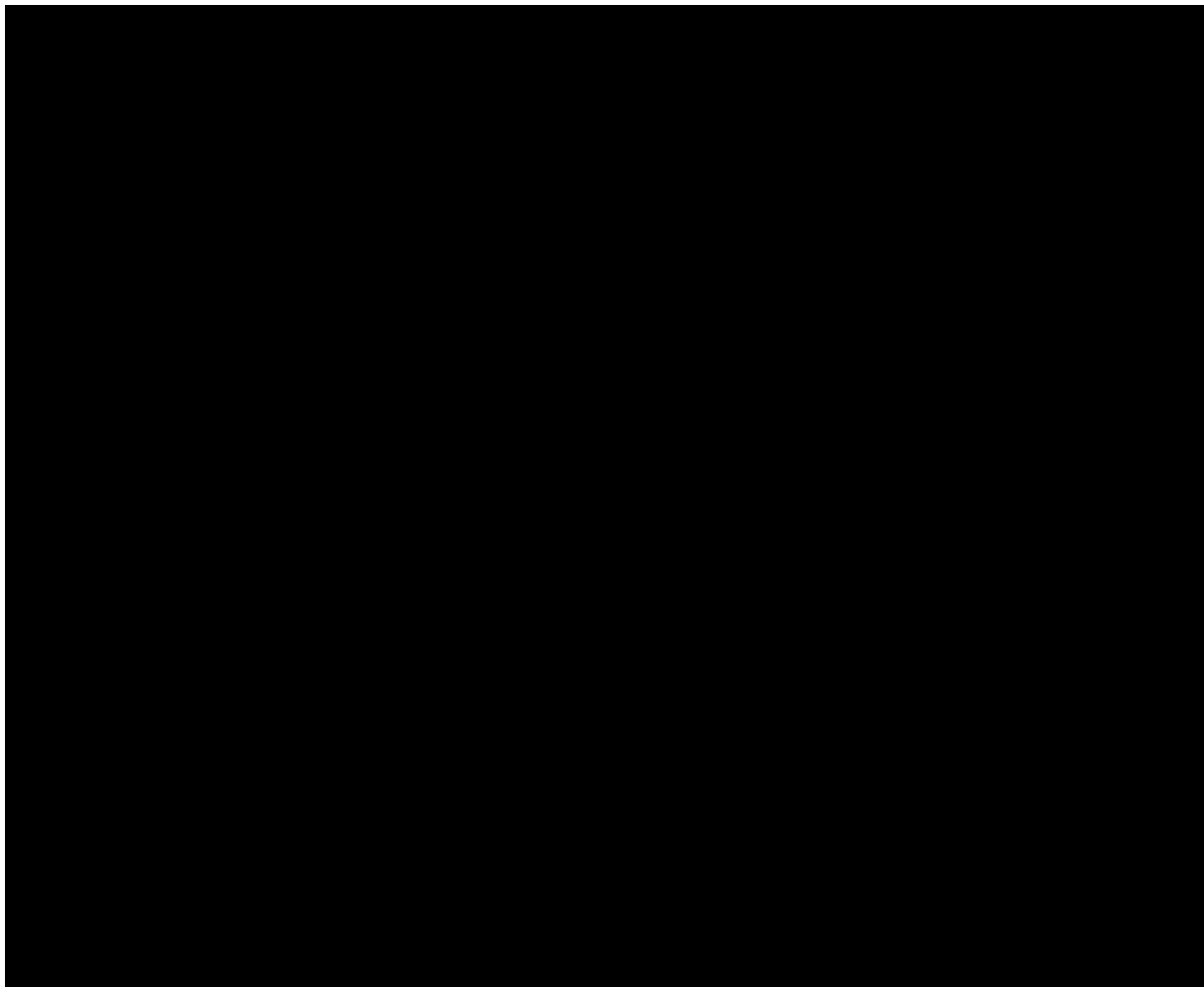
In addition, Oxehealth will provide their best efforts to restore Patient Health Record Data from the backup data held if data becomes corrupted or inaccurate.

6. DPIA Outcomes

The Partnership being proposed between Oxehealth and Essex Partnership University NHS Foundation Trust has the potential to drive improvement in patient safety and care regimes.

Whilst a successful outcome of this nature is desired for the project, the primary focus for Oxehealth and Essex Partnership University NHS Foundation Trust is to ensure respect for the patient and their privacy at all times and that any data generated during the project is processed, transferred, stored or reviewed in a safe and timely manner that complies with Data Protection legislation and any Essex Partnership University NHS Foundation Trust specific local approval processes.

A thorough assessment of the potential risks which might impact a patient's privacy has been undertaken from an Oxehealth Service perspective as well as a detailed review of all data flows and usage in the project. For each risk, a range of proposed solutions has been identified in Section 5 of this DPIA, and it is recommended that each of these be implemented to ensure a successful outcome for the project in terms of patient privacy and data compliance.



Appendix 1

Optional Data Protection Officer sign off form.

The Oxehealth Services Agreement requires that the Essex Partnership University NHS Foundation Trust obtain approval from the Partner's Data Protection Officer for this engagement and the delivery of the Oxehealth Service.

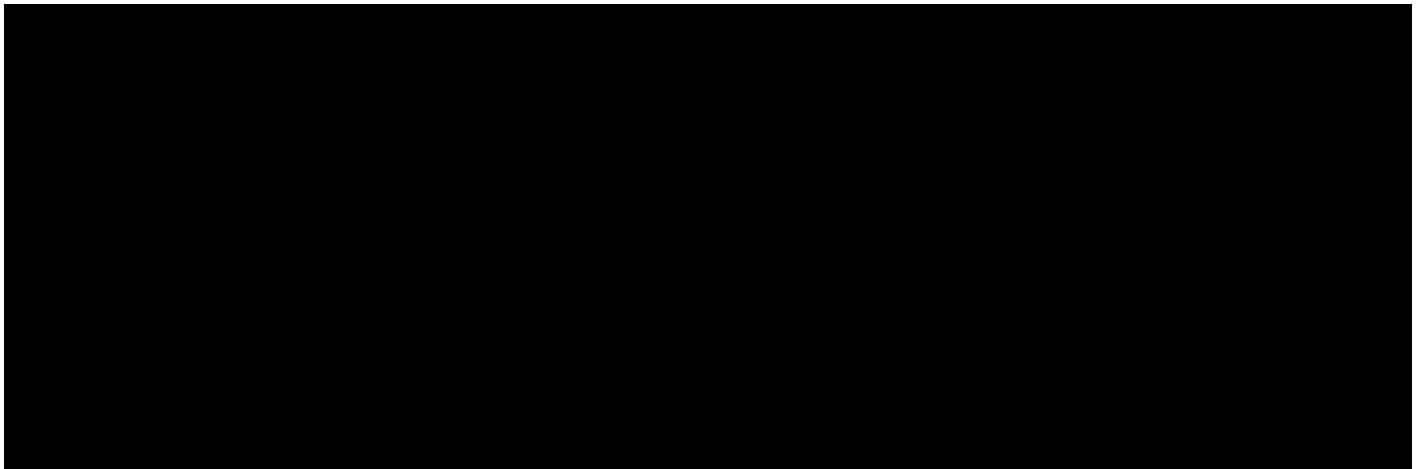
This can be achieved through one of the following methods: (a) using the form set out below (b) the form set out in Schedule 5 of the Oxehealth Services Agreement at the point of contracting for the Oxehealth Service, or (c) otherwise in such other form as may be required by the Partner's internal Caldicott Guardian approval procedures.

If you wish to use the form set out below to evidence the compliance of this Oxehealth – Partner DPIA with GDPR and other data protection and privacy requirements, please complete the following form:

Data Protection Officer Approval

I am the Data Protection Officer for Essex Partnership University NHS Foundation Trust (the "Partner").

I have reviewed Oxehealth's Data Protection Impact Assessment and I am satisfied that it complies with Partner's implementation of GDPR and other data protection and privacy requirements.



Appendix 2

General Data Protection Regulations Principles and Oxehealth's Compliance [Boxed responses]

Source: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/>

Personal data shall be:

- 1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');**

There must be legitimate grounds for collecting Personal Data and it must not have a negative effect on a data subject or be used in a way they wouldn't expect

We are aware that recording people can impact their privacy. The collection of patient healthcare data in the Oxehealth system also impacts their privacy. It is important that any potential infringement on an individual's privacy be in pursuit of a legitimate aim and be proportionate. We consider healthcare and protection of law and order to be legitimate aims for this purpose for these data types, which are both considered to be high risk according to the EDPB. It will not always be necessary to obtain an individual's consent to a course of action that affects their privacy, for example, if the system is used in the normal course of treatment. In line with the Mental Capacity Act it may be that an advocate or the subject's clinical team are able to provide appropriate consents in situations where consent is deemed necessary. We recommend our Partner places signage notifying data subjects of the use of the technology.

Where staff personal data is captured as Staff Identification Data, we consider that this is being processed with the legitimate aim of maintaining an audit trail on the access to and use of other potentially sensitive data within the system. We do not consider this type of personal data to be special category data. Essex Partnership University NHS Foundation Trust determines the legal basis for processing staff information for this purpose and how data subjects will be notified. Oxehealth will support partners to develop staff information leaflets and other materials to help with this.

Where patient identifying information such as patient names or NHS numbers, along with observation records are captured as Patient Health Information, we consider health care to be the legitimate aim for this purpose for this data type. Essex Partnership University NHS Foundation Trust determines the legal basis for processing and how data subjects will be notified. Oxehealth will support partners to develop patient information leaflets and other materials to help with this.

- 2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');**

Data should be collected for specified and explicit purposes and not be used in a way someone wouldn't expect

The purpose for which the Oxehealth system is being used by Essex Partnership University NHS Foundation Trust is clearly and transparently laid out in the contract between Oxehealth and that Partner; this Data Protection Impact Assessment sets out the controls and processes implemented by

Oxehealth to ensure data processing is only undertaken in a way compatible with this purpose.

Clear Video Data is personal data, and is needed to fully debug the system or enable additional investigations to improve project functionality. The use of Clear Video Data is kept to a minimum, used only when Essex Partnership University NHS Foundation Trust wants to bring something to the attention of Oxehealth in order to improve functionality or Oxehealth's engineers identify sections requiring analysis and Essex Partnership University NHS Foundation Trust instructs Oxehealth to investigate.

Patient Health Record Data is personal data, and is needed to provide the Oxevision Observations functionality desired by Essex Partnership University NHS Foundation Trust to assist in providing patient care. This data and Staff Identification Data (also personal data) are collected to provide this service and provide Essex Partnership University NHS Foundation Trust with the capability to audit collection and modification of personal data to support their role as Data Controller. Data collection is kept to the minimum required and data retention is reduced as far as is possible to provide the software service. Oxehealth staff are not required to access patient names, health record data or medical history. They are only given access to maintain or restore the software service and will not have access to any of this data in a decrypted form.

All other data collected and processed as part of this project is anonymised and non-personally identifiable.

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

It must be clear why the data is being collected and what will be done with it. Unnecessary data or information without any purpose should not be collected

Personal data collection is as per 2 above.

The collection of this is kept to a minimum and only used in order to fully debug the system or enable additional investigations as instructed by Essex Partnership University NHS Foundation Trust to improve project functionality.

The Collection of Patient Health Record Data and Staff Identification Data is kept to the minimum required to provide the service and enable Oxehealth to maintain and restore the software service without ever accessing decrypted personal data.

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

Personal data collection is as per 2 above.

Clear Video Data is reviewed only in order to fully debug the system or enable additional investigations [as instructed by Essex Partnership University NHS Foundation Trust to improve project functionality. With the exception of anonymising facial and other personally identifiable features where clipped

Personally Identifiable Video Data is retained for ongoing investigation and testing, no changes to the raw video data are made by Oxehealth software or Oxehealth staff, with integrity controls on the raw images and their transport, and access controls and modification controls on the Oxehealth storage systems, maintaining the accuracy required.

Patient Health Record Data is created and modified by Essex Partnership University NHS Foundation Trust staff, and may be either entered inaccurately, or be subject to modification. Essex Partnership University NHS Foundation Trust must ensure that accuracy is maintained and Oxehealth has provided the audit record including Staff Identification Data to assist in maintaining accuracy. Patient Health Record Data is not altered by Oxehealth software or staff after storage.

Staff Identification Data required for Oxevision Observations is collected only to provide user authentication and audit trail of personal data creation and modification. No changes to the Staff Identification Data are made by Oxehealth software or Oxehealth staff, maintaining the accuracy required.

5. 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; ('storage limitation');

Personal data collection is as per 2 above.

The collection of Clear Video Data is kept to a minimum and only used in order to fully debug the system or enable additional investigation as instructed by Essex Partnership University NHS Foundation Trust to improve project functionality where this cannot be achieved with non-personal Anonymised Video Data and Algorithm Debug Data. Clear Video Data is deleted once these tasks have been fully completed.

Patient Health Record Data and Staff Identification Data required for Oxevision Observations is stored only for as long as is required to provide the software service function required by the Partner. Data held in the software on site is deleted at the end of the useful period to the users and backup data to enable service restoration is deleted as soon as is reasonably possible.

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Non-compliance with Principle 6 is a key risk for Oxehealth with full details of the approach taken to compliance laid out in Sections 3 and 5 of the DPIA.

7. transferred to other countries only where either UK "adequacy regulations" or exemptions exist, or where appropriate risk assessment and safeguards have been put in place.

All data generated by the Oxevision system is stored on local secure servers at Essex Partnership University NHS Foundation Trust 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, a Sweden data centre for Swedish Partners, and a US data centre for US Partners.

Where Oxehealth is instructed to transfer Clear Video Data 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, there European Commission's adequacy decision for data transfers to the UK under the EU GDPR says that the UK provides adequate protection for 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 Partners of these providers