

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.

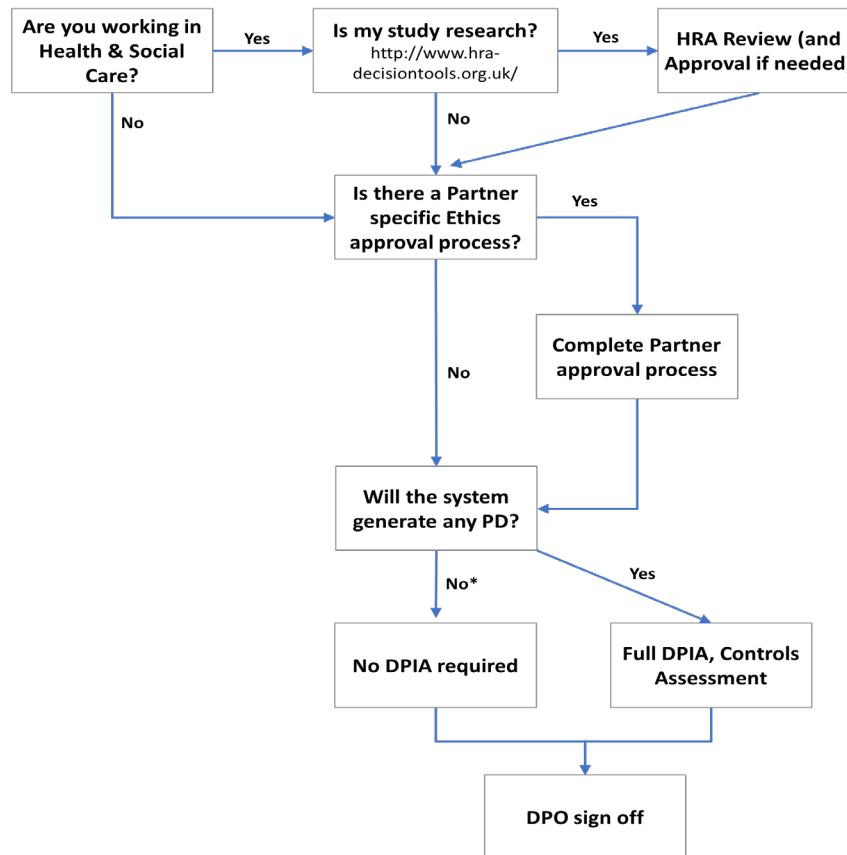
In this project, Essex Partnership University NHS Foundation Trust wishes to deploy the Oxehealth Software & Oxehealth Services to improve and supplement its patient care and safety monitoring regimes.

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

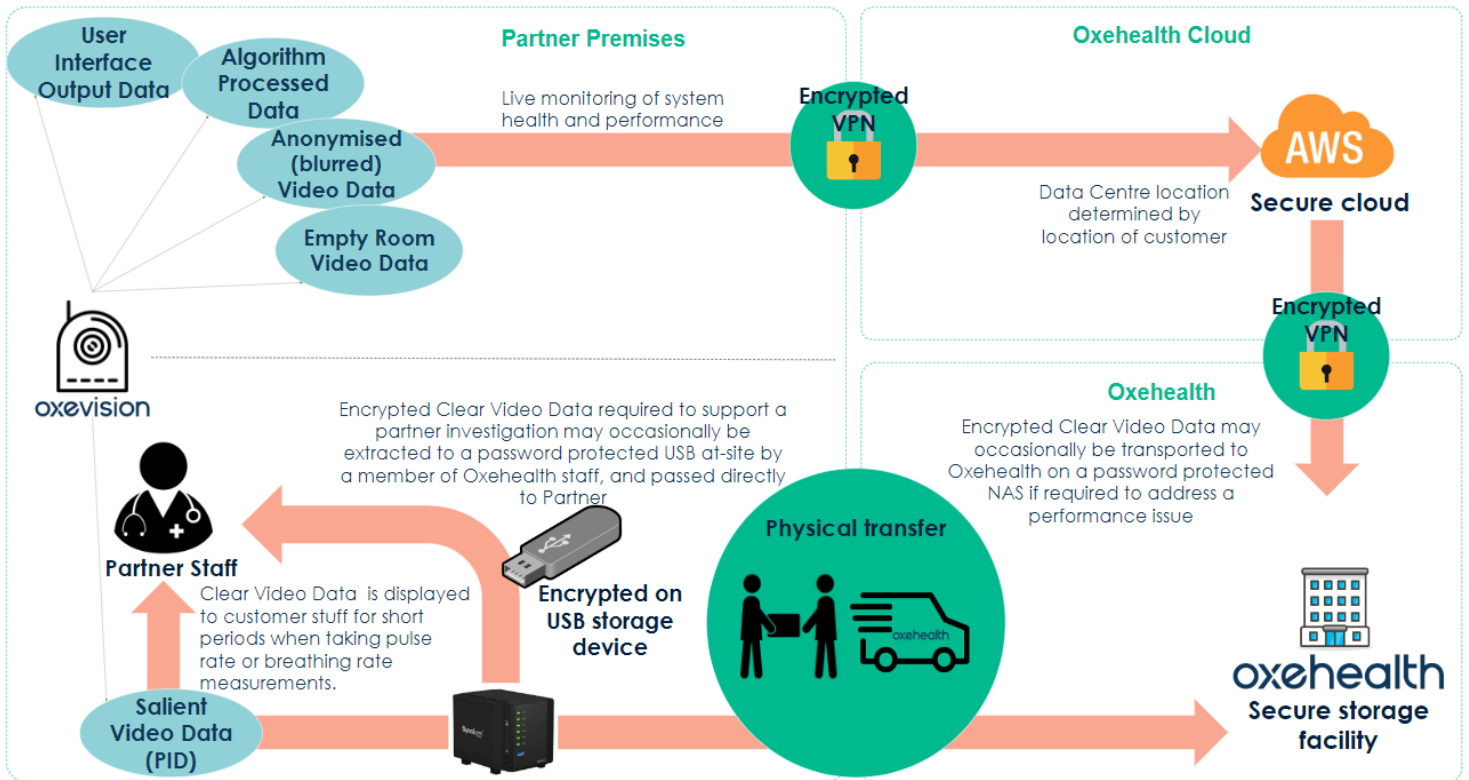


Figure 1. Data Flows from the Oxevision software on Partner Premises to Oxehealth

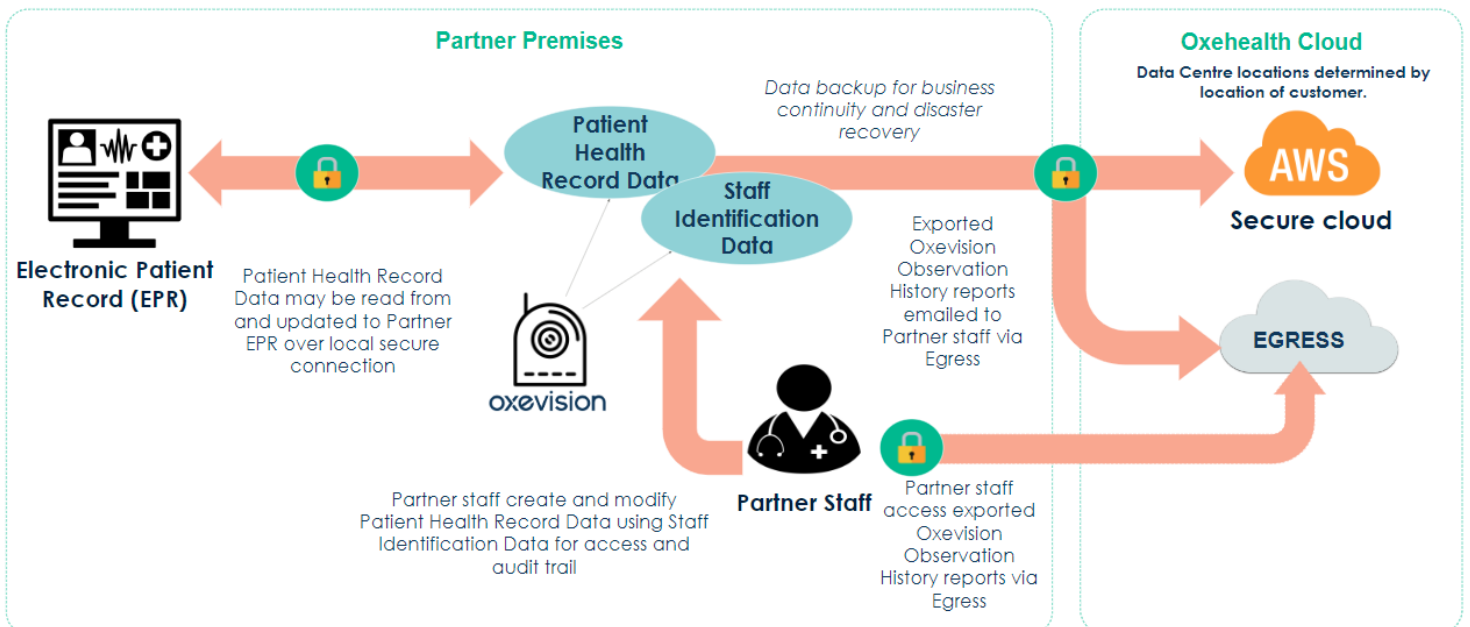


Figure 2. Data Flows from the Partner Electronic Patient Record (EPR) and the Oxevision Observations software on Partner Premises to Oxehealth

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.

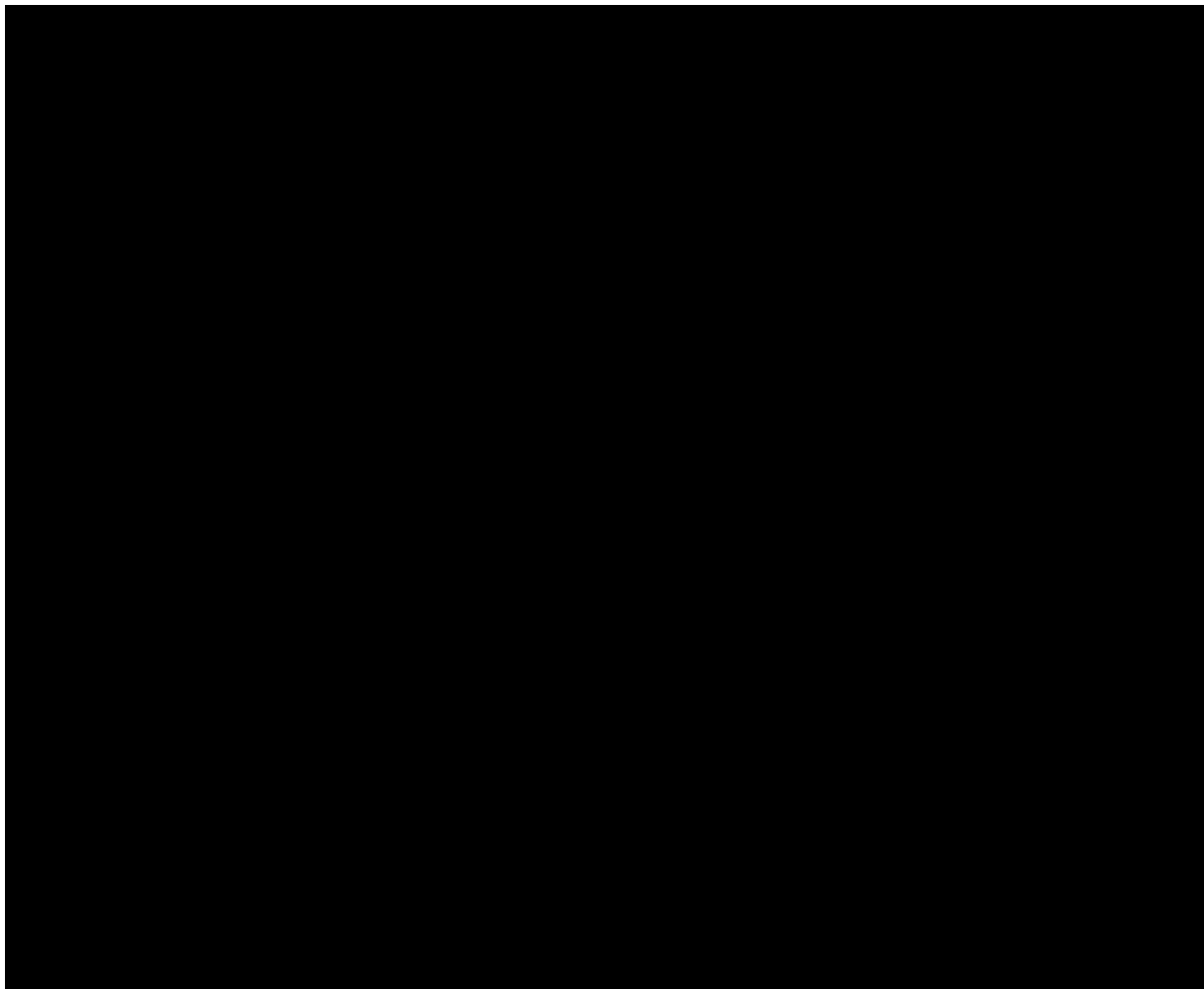
In addition, Oxehealth will provide their best efforts to restore Patient Health Record Data from the backup data held if data becomes corrupted or inaccurate.

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.

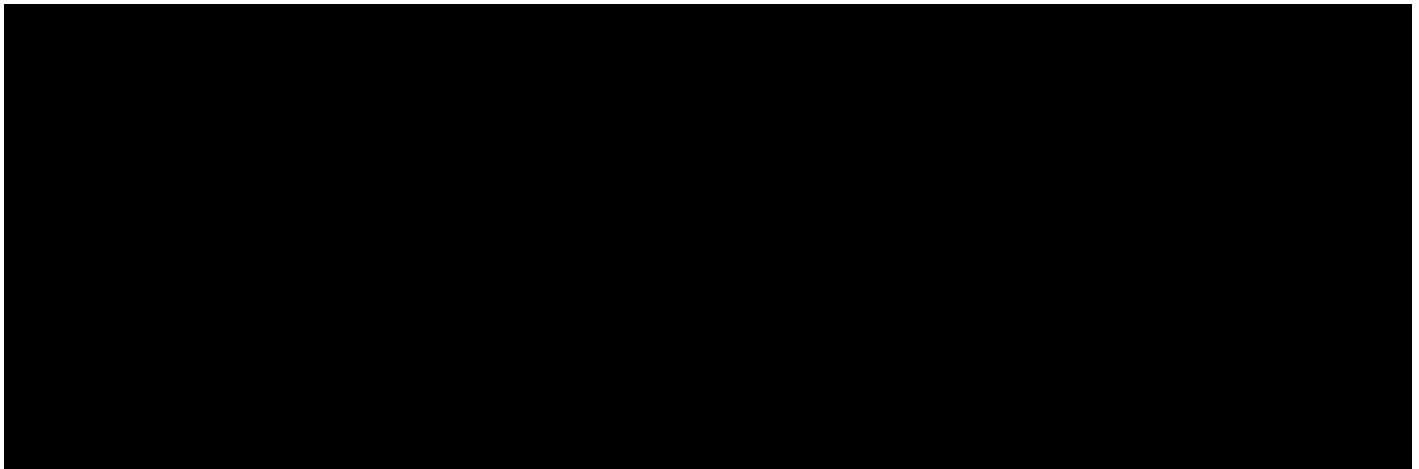
This can be achieved through one of the following methods: (a) using the form set out below (b) the form set out in Schedule 5 of the Oxehealth Services Agreement at the point of contracting for the Oxehealth Service, or (c) otherwise in such other form as may be required by the Partner's internal Caldicott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