**Data Protection Impact Assessment (DPIA)
Template**

A Data Protection Impact Assessment (DPIA) must be completed whenever a new service, process or information asset is introduced or there is a change to an existing process or service. Steps 1 – 3 must be completed for all projects / proposals. If advised to do at the end of Step 3 please complete Step 4. Completed DPIAs should be emailed to elft.information.governance@nhs.net

Step 1. Project / proposal details *Complete for all projects / proposals*

Project / proposal name: Oxehealth Digital Care Assistant
Description of project / proposal: Explain broadly what project aims to achieve and what type of processing it involves. Please attach a document or link to other documents, such as a project proposal if you have one. Is it a new electronic system, service acquisition, software, information sharing proposal or something else? 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. East London 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 – Edge of Bed, Out of Bed, Out of Room, Multiple People, Dwelling in en suite bathroom timer - Activity Report - Vital Signs Trend Report In this project, East London NHS Foundation Trust wishes to deploy the Oxehealth Software & Oxehealth Services to improve and supplement its patient care and safety monitoring regimes.
Give an overview of the processing: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? Attach a flow diagram or describe data flows. What types of processing identified as likely high risk are involved?

Is a supplier involved in the processing? If the supplier is known at this stage, give supplier details – attach evidence of DSPT accreditation, BS27001 accreditation or otherwise copies of their information security policies, evidence of IG training etc

Oxehealth
Magdalen Centre North
Oxford Science Park
Oxford
OX4 4GA

Oxehealth is ISO13485 and ISO27001 certified, and Oxehealth holds the UK Government Cyber Security Plus certification and is audited against these certifications.

Oxehealth holds the DCB0129 information standard, has completed the Data Security & Protection Toolkit (DSPT) with "standards exceeded" and is ICO registered.

PDF	PDF	PDF
Cyber Essentials Plus Certificate.pdf	ICO Data Protection Registration Certifica	ISO270001.pdf

What are the benefits?

The key benefits of the Oxehealth system for seclusion are:
1. Ability to get Medically Certified *(Class IIA Medical Device Certification (BSI ISO 13485))* spot check vital signs (pulse rate and breathing rate) from patients in a seclusion environment without having to enter the seclusion environment providing improved adherence to physical health monitoring, e.g. post-rapid tranquilisation/new admissions
2. Activity Detection – system will alert when no activity is detected for 30 seconds or longer which may indicate that a patient has stopped breathing
3. Earlier detection of physical health deterioration
4. Access to history report of observations taken which provides a view of the progress of a patient over time.
5. Monitoring of patient movement within the seclusion environment including bathroom entry/exit.
6. The system will alert (audible and visual alert) if a patient is in the bathroom longer than a pre-defined time
7. Monitoring of number of room entry/exits
8. Improved confidence in managing patient risk and improved sense of safety and privacy
9. More information to support patient care and medication intervention
10. Ability to review video evidence of alerts/incidents and include video evidence in incident reports (under strict governance)
11. Objective data on patient movement and vitals monitoring

Wider scope of benefits includes:

Benefit	Strategic Agenda	Desired Outcome	Services Applicable	Key Metrics
Safer patient care	Safety & Quality	o Reduced falls in bedrooms o Reduced severity of falls in bedrooms o Reduced demand for	Older Adult	o Incident reports o Staff surveys

			Ambulance services and A&E attendance		and interviews
Safer patient care	Safety & Quality	o Reduced incidences or early warnings to violence/aggression, self-harm (e.g. ligatures) o Earlier warnings to contraband and smoking related incidents	PICU	o Incident reports o Staff surveys and interviews	
Safer patient care	Safety & Quality	o Undisturbed night observations	All	o Staff surveys o DCA system data	
Safer patient care	Safety & Quality	o Improved adherence to physical health monitoring, e.g. post-rapid tranquillisation, new admissions o Earlier detection of physical health deterioration	All, especially seclusion & S136 suites	o Physical health monitoring o Incident reports o Staff surveys	
Better patient experience	Safety & Quality	o Improved sleep quality, sense of safety and privacy	All	o Patient feedback	
Better staff experience	Safety & Quality, Recruitment, Retention	o Improved confidence in managing patient risk, improve sense of safety and peace of mind	All	o Staff surveys and interviews o Staff morale o Staff sickness & absence	
More effective care	Safety & Quality	o More information to support patient care & medication interventions	All	o Staff surveys and interviews	
Objective, auditable data	Governance	o Objective data on patient activity and vital signs o Objective video data & reports for serious incidents (under strict governance) o Audit trail o Reduced cost for litigation	All	o n/a	
Saved clinical time	Operational, Financial	o Reduction in time spent on avoidable enhanced observations o Reduction in time spent on non-direct care activities o Faster L1 and L2 observations at night	All	o Enhanced observation hours o Agency/bank spend o Staff surveys and interviews o Time-and-motion study	

Proposed implementation date:

As soon as possible

Step 2. Contact details *Complete for all projects / proposals. Please contact the IG team if anything is unclear*

Work stream lead / project manager details	
Name ██████	**Job title** **Medical Devices Lead**
Email ████████████	**Phone** ████████

Information Asset Owner (if different from above). This will be a Service Director, Corporate Director / Associate Director	
Name ███████	**Job title** **Deputy Director Of infection Control**
Email ████████████	**Phone** ███████

Information Asset Administrator (or System Owner). This will usually be a team manager, IT super user etc	
Name 	**Job title**
Email 	**Phone**

Executive Director sponsor details. Required for large scale change, acquisitions etc, not for small projects	
Name ██████	**Job title** Director of Nursing (London Mental Health)
Email ██████████	**Phone** ███████

Step 3. Screening questions. *Complete for all projects / proposals*

Answering YES to any of the screening questions represents a potential high risk to the rights and freedoms of individuals and therefore a full DPIA must be completed to ensure those risks are identified, assessed and fully mitigated.

Screening questions	Yes or No
Will the project / proposal involve the collection / processing of information about individuals? (this could be service users, carers, staff, stakeholders etc)	Yes
Does it introduce new or additional information technologies that can substantially reveal business sensitive information / have a high impact on the business?	Yes
Will it require individuals to provide information about themselves?	No
Will information about individuals be disclosed to organisations / individuals who have not previously had routine access to the information?	Yes
Will information about individuals be used for a new purpose or in a new way?	Yes
Does it use technology that could be seen as intrusive e.g. automated decision making?	Yes
Will it result in making decisions about individuals that may have an impact on them e.g. research, service planning, commissioning new services?	No
Will it change the delivery of an individual's direct care?	Yes
Will it require you to contact individuals in a way they might find intrusive?	No
Does it involve any other organisations?	No
Does it require individuals to consent to their information being processed?	No
Does it involve new or significantly changed handling of a considerable amount of personal / business sensitive information about an individual in a database or system?	Yes
Does it involve new or significantly changed consolidation, interlinking, cross referencing, or matching of personal / business sensitive data?	No
Does it use cloud services / is it stored in 'the cloud'?	Yes
Is it about children or vulnerable groups of adults e.g. service users?	Yes
Will it be used for research purposes / projects?	No

If you answered YES to any of the above questions please complete Step 4. If you answered NO to all questions then please send your DPIA to elft.information.governance@nhs.net. We will assess your request and either confirm our data protection support for your project / proposal or request further information. Please contact the IG team if anything is unclear.

Step 4. Full Data Protection Impact Assessment *Complete only when advised a full DPIA is necessary at the end of Step 3*

4.1 Processing

What data will be collected / processed? Does it include health or any other special categories of data? If so, please list. These are health, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

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 an "Oxeroom" installation with the data stored in a securely encrypted format. This encrypted data is 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 stored on secure remote servers based in the UK.

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

Non-Personal Data

a) Anonymised Video Data - 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 Video Data. Oxehealth will also compress and encrypt this feed and transfer it securely to its secure remote UK servers. Anonymised Video Data is required to ensure the Oxehealth Service delivers the Contract Purpose to the contracted standard. The Anonymised Video Data cannot be viewed by unauthorised persons because it is encrypted and – even were it decrypted - the anonymisation prevents individuals 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 ensure the Oxehealth Service delivers the Contract Purpose to the contracted standard. These data are also encrypted and sent to Oxehealth's secure remote UK servers. These data cannot be used to identify an individual.

c) User Interface Output 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 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 Partner'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.

Anonymised Video Data, Algorithm Processed Data and User Interface Output Data ("Non-Personal Data") do not constitute personal data in circumstances where Oxehealth does not have access to Salient Video Data in respect of the same footage.

Personal Data

Salient Video Data – 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 medical device certification. Other modules may offer the option of setting up a raw video feed in response to a user action, at the discretion of Partner when specifying system set up. The Oxeserver also stores encrypted raw video data on a [24 hour] "rolling buffer", meaning that encrypted video from each room is held securely for [24 hours] before being recorded over and becoming irrecoverable.[1] The raw video for these periods is called Salient Video Data. Salient Video Data which contains images of staff, patients or other personnel is personal data. This is referred to as "Personally Identifiable Salient Video Data". Salient Video Data which does not contain images of staff, patients or other personnel is not personal data. In contrast to Anonymised Video Data, Salient Video Data is encrypted but not anonymised because the identifiable 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.

Salient Video Data may be "clipped" (marked for retention on the Oxeserver so that it is not recorded over) by Oxehealth remotely, and transported to Oxehealth's facilities from time to time. See "C. Usage of Data at Oxehealth" below for usage of Salient Video Data.

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

How will the data be collected?
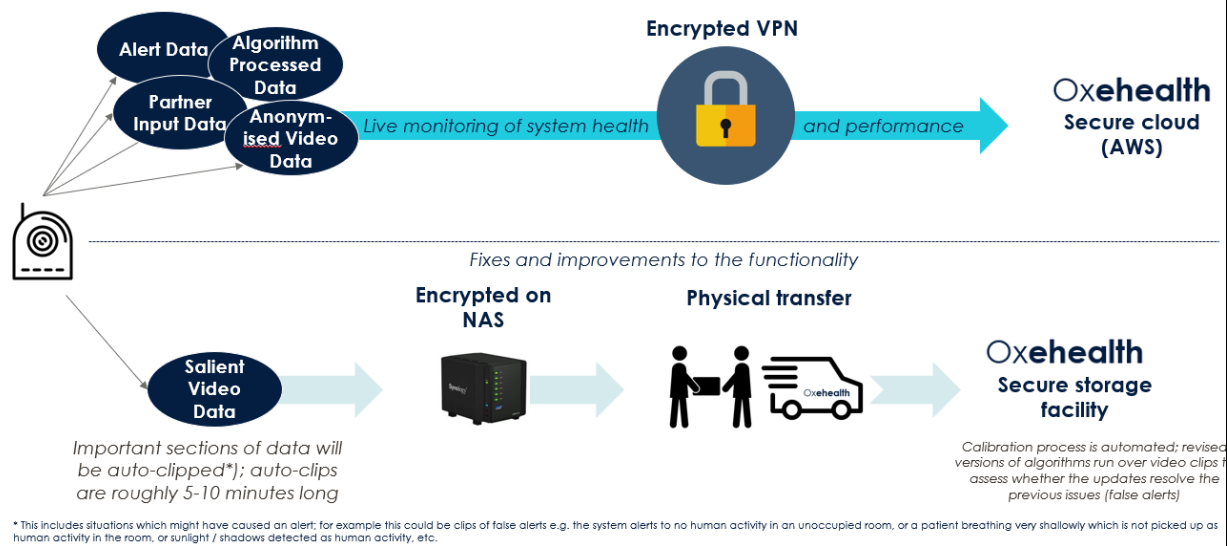
Data will be collected from every Oxeroom installation and is transferred, in an encrypted format via

---

[1] Note: The rolling buffer may vary from a minimum of 24 hours up to approximately 72 hours.

Ethernet cabling, to the Oxeserver, located in a secure Partner facility.

The Oxehealth Software modules hosted on Oxeserver are accessed by staff through fixed monitors located securely on Partner's premises or through dedicated tablets through a secured, encrypted wi-fi connection.

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 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 the Partner as per the contracted standard.

To deliver the service to the contracted standard, on occasion, Oxehealth need to obtain a "reference image" of a room via the internet. A "reference image" is images of an empty room over a 60 second period that do not contain any personal data. Prior to transferring the "reference image", Oxehealth verifies that there is no personal data contained within the image by cross-checking Anonymised Video Data and Algorithm Processed Data to ensure no individuals are present. Once this is confirmed, Oxehealth's internal process requires two separate, internal sign offs before the "reference image" can be transferred: Systems Team sign-off and Executive Team sign-off.

All 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

Personally Identifiable 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 agreed prior to the transfer with East London NHS Foundation Trust in writing) 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.

Where will it be collected from?

See above

What will it be used for?

Non-Personal Data

As set out above, the vast majority of data used in the project is not personally identifiable. Anonymised Video Data, Algorithm Processed Data and User Interface Output Data do not constitute personal data in circumstances where Oxehealth does not have access to Salient Video Data in respect of the same footage (the "Non-Personal Data").

Oxehealth only uses Non-Personal Data for the purpose of providing the Oxehealth Service to the Partner.

Non-Personal Data is deleted following expiry or termination of the agreement between Oxehealth and the Partner.

Personal Data

As set out above, Salient Video Data may be "clipped" and transported to Oxehealth's facilities from time to time. Data is clipped for two reasons.

First, Oxehealth may clip empty room Salient Video Data (i.e. does not contain images of people) from time to time to ensure there are no local phenomena which could prevent Oxehealth from delivering the Contract Purpose to the contracted standard (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 Video Data and Algorithm Processed Data.

Second, Oxehealth may clip Salient Video Data containing images of people ("Personally Identifiable Salient Video Data"). This data is personal data. This clipping process is triggered by Partner staff or Oxehealth in one of three ways:

1. By a member of the Partner's staff who believe that they have identified something in the functioning of the system which they wish to bring to the attention of Oxehealth's engineers in order to ensure the Oxehealth Service delivers the Contract Purpose to the contracted standard
2. By Oxehealth flagging data that they believe should be reviewed to ensure the Oxehealth Service delivers the Contract Purpose to the contracted standard
3. By a member of the Partner's staff flagging the need to store data to support an internal or external investigation (for example, into a suspected serious adverse event).

Much of the data analysis on Salient Video Data for the Contract Purpose will be performed automatically, using computers, over Salient Video Data and Anonymised Video Data.

From time to time, Oxehealth's engineers may need to review a short period of Salient Video 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.

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 Salient Video Data will be used for marketing, or publicity purposes.

The Personally Identifiable Salient Video Data will only be kept for as long as is needed to answer queries raised by East London NHS Foundation Trust staff or by engineers at Oxehealth. To support this, all data files are date and time stamped so that retention can be tracked.

Oxehealth undertakes periodic reviews with the Partner to consider the Personally Identifiable Salient Video Data held, the reason for the data retention and confirmation of Personally Identifiable Salient Video Data deleted.

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 personal data retained, reasons for retentions and date of next review. Oxehealth will process all personal data generated in the project in accordance with this DPIA and documented instructions from East London NHS Foundation Trust, the Data Controller.

Salient Video Data will be securely deleted at the end of the project or when no longer required, whichever is the earlier. In addition, East London NHS Foundation Trust have the ability to request that Oxehealth delete Personally Identifiable Salient Video Data at any time.

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.

Will it be processed manually? Yes or No

No

Will it be processed electronically? Yes or No   Yes

How is access controlled? For example passwords, Smartcard, locked door   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 UK 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 securely at East London 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.

Will only the minimum data necessary be collected / stored / processed?   Yes

Will be anonymised, pseudonymised or collated with other data?   No

Will any third parties access the data? Who? For example if another organisation wants access to our systems   No

Will it be sent off site or shared externally i.e outside the Trust or outside its computer network? Yes or No   Yes

If sent off site, where to? Name the other agency / company / location / country

Salient Video Data – 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 medical device certification. Other modules may offer the option of setting up a raw video feed in response to a user action, at the discretion of Partner when specifying system set up. The Oxeserver also stores encrypted raw video data on a [24 hour] "rolling buffer", meaning that encrypted video from each room is held securely for [24 hours] before being recorded over and becoming irrecoverable.[2] The raw video for these periods is called Salient Video Data. Salient Video Data which contains images of staff, patients or other personnel is personal data. This is referred to as "Personally Identifiable Salient Video Data". Salient Video Data which does not contain images of staff, patients or other personnel is not personal data. In contrast to Anonymised Video Data, Salient Video Data is encrypted but not anonymised because the identifiable 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.

Salient Video Data may be "clipped" (marked for retention on the Oxeserver so that it is not recorded over) by Oxehealth remotely, and transported to Oxehealth's facilities from time to time. See "C. Usage of Data at Oxehealth" below for usage of Salient Video Data.

Salient Video Data is held separately to the Anonymised Video Data, Algorithm Processed Data and User Interface Output 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).
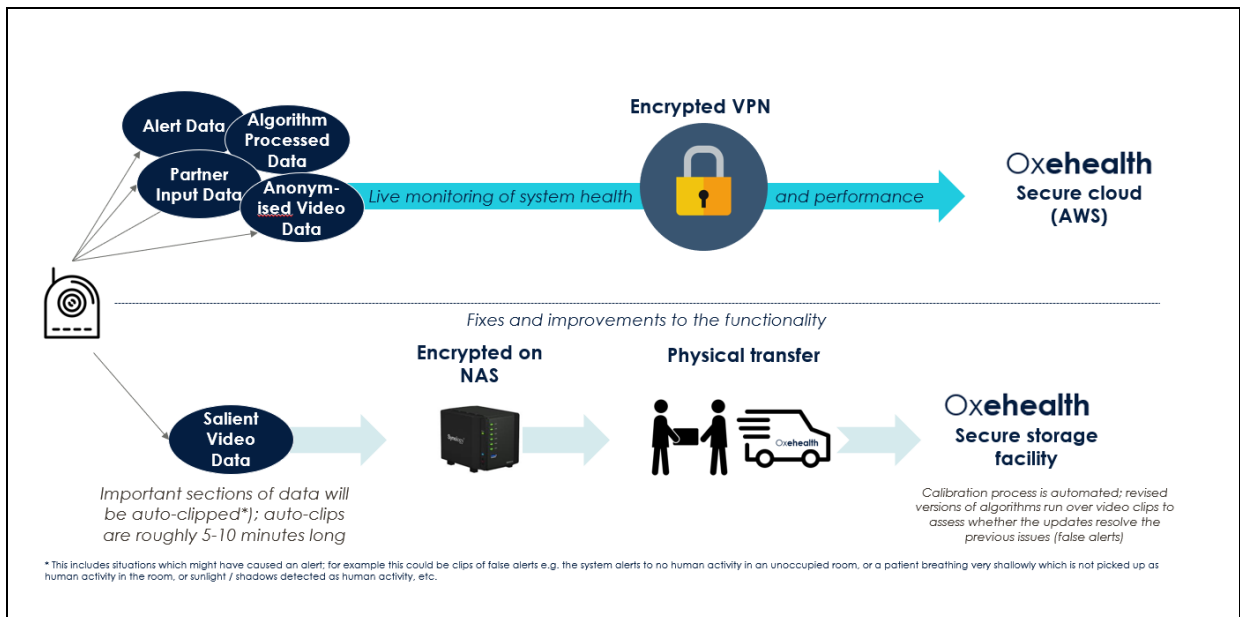
This data is stored physically on secure servers in the UK and Oxehealth has no intention of moving its business, or this data, outside of the UK.

If so, is there a contract / data controller to processor agreement, information sharing agreement? If yes, please attach

There is a contract that covers this.

How will it be sent?

---

[2] Note: The rolling buffer may vary from a minimum of 24 hours up to approximately 72 hours.

Live monitoring of system health and performance

Fixes and improvements to the functionality

Important sections of data will be auto-clipped*); auto-clips are roughly 5-10 minutes long

Calibration process is automated; revised versions of algorithms run over video clips to assess whether the updates resolve the previous issues (false alerts)

* This includes situations which might have caused an alert; for example this could be clips of false alerts e.g. the system alerts to no human activity in an unoccupied room, or a patient breathing very shallowly which is not picked up as human activity in the room, or sunlight / shadows detected as human activity, etc.

How long will the data be retained in identifiable form?   As long as permitted by ELFT – all data held will be regularly reviewed and ELFT can instruct any data to be deleted at any time.
Will it be de-identified or destroyed. How?   Identifiable data will be destroyed if instructed to do so.
Are you aware of any concerns or risks over the processing / use of the data, system, supplier, other agency etc?   No
Has any / will any consultation take place? Yes or No? Please list, also include feedback received   ??NOT SURE WHAT IS MEANT BY THIS QUESTION – WHAT IS MEANT BY CONSULTATION??

4.2 Cloud considerations. You must complete this if you answered Yes in Step 2 to 'Does it use cloud services / is it stored in 'the cloud'?
Which country is the cloud provider based in? England
Is the cloud service hosted on HSCN? Yes
What business continuity plans are in place if the provider ceases trading? Covered in contract
What secure arrangements are in place at the end of the contract with the cloud provider to transfer the data? Covered on contract.
Who would legally own any data uploaded to the cloud application by the Trust? ELFT owns all right, title and interest in the Salient Video Data, Anonymised Video Data and User Interface Output Data. Oxehealth owns all right, title and interest in the Algorithm Processed Data. For the avoidance of doubt, Algorithm Processed Data constitutes Oxehealth Confidential Material.
What information & cyber security policies does the cloud provider have? Please attach information / embed a link Oxehealth is ISO13485 and ISO27001 certified, and Oxehealth holds the UK Government Cyber Security Plus certification and is audited against these certifications. Oxehealth holds the DCB0129 information standard, has completed the Data Security & Protection Toolkit (DSPT) with "standards exceeded" and is ICO registered. Cyber Essentials Plus Certificate.pdf   ISO270001.pdf

Please send your completed DPIA to elft.information.governance@nhs.net. We will assess your request and either confirm our data protection support for your project / proposal or request further information.

Information Governance assessment

To be completed by the information governance team who will advise you once the assessment is complete
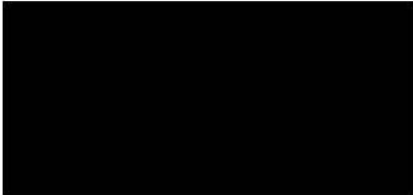
Compliance area	Assessment of compliance	Compliance agreed by IG Manager Y / N
Principle 1 Lawfulness, fairness and transparency Transparency: Are data subjects aware what data processing will be done? Fair: Is the processing as described? Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)], that personal data shall be: "(a) processed lawfully, fairly and in a transparent manner in relation to individuals	The Legal basis for processing is Article 6 (c) Legal obligation, read in conjuction with the Health and Social Care act and Article 9 (2)(h).	Y by DPO
Principle 2 Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Is the data only being used for the specific processing purpose that the subject has been made aware of?	Data will only be processed to support patient safety monitoring	Y by DPO
Principle 3 Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. Is only the minimum amount of data kept for specific processing?	Data is limited to vital signs observations and monitoring	Y by DPO
Principle 4 Personal data shall be accurate and, where necessary, kept up to date. [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Are there rectification processes in the data management / archiving activities	Retention periods are clearly defined and stored for limited periods	Y by DPO
Principle 5 Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. Is this recognised and what processes are in place to ensure it happens?	Company has clear processes in place for managing personal data	Y by DPO

Principle 6 Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage" [article 5, clause 1(f)]. Is the security adequate? Is there a system level security policy?	Company is ISO 27001 and Cyber Essentials Plus certified	Y by DPO
Information sharing Is an information sharing or third party access agreement required? Y/N	No	Y by DPO
Cloud considerations Has the Information Security Manager approved the Cloud section? Y/N	ICT involved in rollout	Y by DPO
Risks Assess the source of risk & nature of potential impact on the rights & freedoms of individuals. Include associated compliance & corporate risks as necessary	(risk matrix below)	
Asset register / data flows mapping Has the asset been added to the relevant asset register? Y/N	To be added	

Risk matrix:

Severity	Likelihood				
	1	2	3	4	5
	Rare	Unlikely	Possible	Likely	Almost
5	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Negligible	1	2	3	4	5

Is the risk great enough to report to the ICO? N

Add comments:

Likelihood = 2
Severity = 3
Risk = 6

Information governance team to forward to DPO

Data Protection Officer approval

DPO comments Project underway prior to information governance involvement therefore DPIA done retrospectively, supported by DPIA supplied by provider

DPO approval granted? Y/N Yes
DPO name: ██████████
DPO signature: ████████████
DPO approval date: 07.01.2021

DPO to return form to information governance team for documenting and returning to project manager

Date returned by IG team to project manager: