Our Ref: NG/RM/24125
Date: 2nd May 2024

Nicola Griffiths
Deputy Director of Governance
North Staffordshire Combined Healthcare NHS Trust
Lawton House
Bellringer Road
Trentham
ST4 8HH

Reception: 0300 123 1535

Dear

Freedom of Information Act Request

I am writing in response to your e-mail of the 3rd April 2024**.** Your request has been processed using the Trust's procedures for the disclosure of information under the Freedom of Information Act (2000).

Requested information:
I would like to request a copy of any Data Protection Impact Assessments the Trust has relating to the use of Oxevision or other Oxehealth technology. If it is not clear from the documents themselves, please provide the approximate dates when they were last updated and when they were last reviewed.

Please see Appendix 1 attached.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review of the management of your request. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Dr Buki Adeyemo, Chief Executive, North Staffordshire Combined Healthcare Trust, Trust Headquarters, Lawton House, Bellringer Road, Trentham, ST4 8HH. If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

Nicola Griffiths
Deputy Director of Governance

Confidential

Oxehealth

Data Protection Impact Assessment

NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST

October, 2021

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. However, 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

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.

NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST (or Partner) is a leading provider of mental health, social care, learning disability and substance misuse services in the West Midlands.

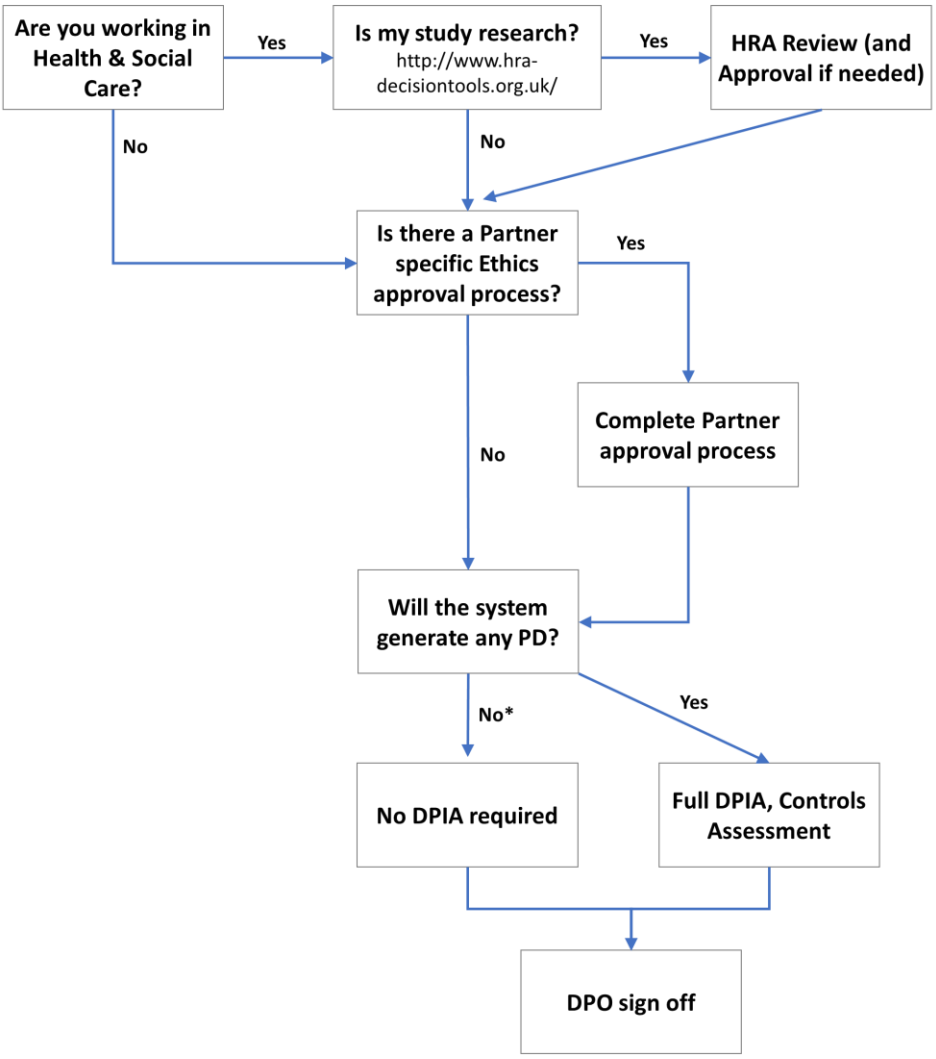
NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST is procuring the following Oxehealth software modules:

- Oxehealth Vital Signs (a Class IIa medical device in Europe)
- Activity Detection for Seclusion
- High Risk Activity Alerts/Warnings – Edge of Bed, Out of Bed, Out of Room, Multiple People, Dwelling in en-suite bathroom timer
- Activity Report
- Vital Signs Trend Report (a Class IIa medical device in Europe)

In this project, NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST wishes to deploy the Oxehealth Software & Oxehealth Services to improve and supplement its patient care and safety monitoring regimes [Contract Purpose].

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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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 **[tbc with Partner]**	-
Will the system generate any Personal Data?	Yes	Full DPIA and Controls Assessment needed
Are there any NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST specific Data Holding requirements?	No **[tbc with Partner]**	-

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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST.
- **Systematic monitoring (EDPB risk trigger):** Whilst CCTV is used throughout NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST facilities and in seclusion rooms, it is not currently used in the patient bedrooms proposed to be used for the project. In this project, digital video cameras will be used to record and process the data to potentially help NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST improve its current patient safety and activity monitoring regimes.
- **Sensitive data or data of a highly personal nature (EDPB risk trigger):** The system captures health data (including vital signs) regarding patients under the care of NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST.
- **Data concerning vulnerable data subjects (EDPB risk trigger):** The data subjects are patients at NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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 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 or still images 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.

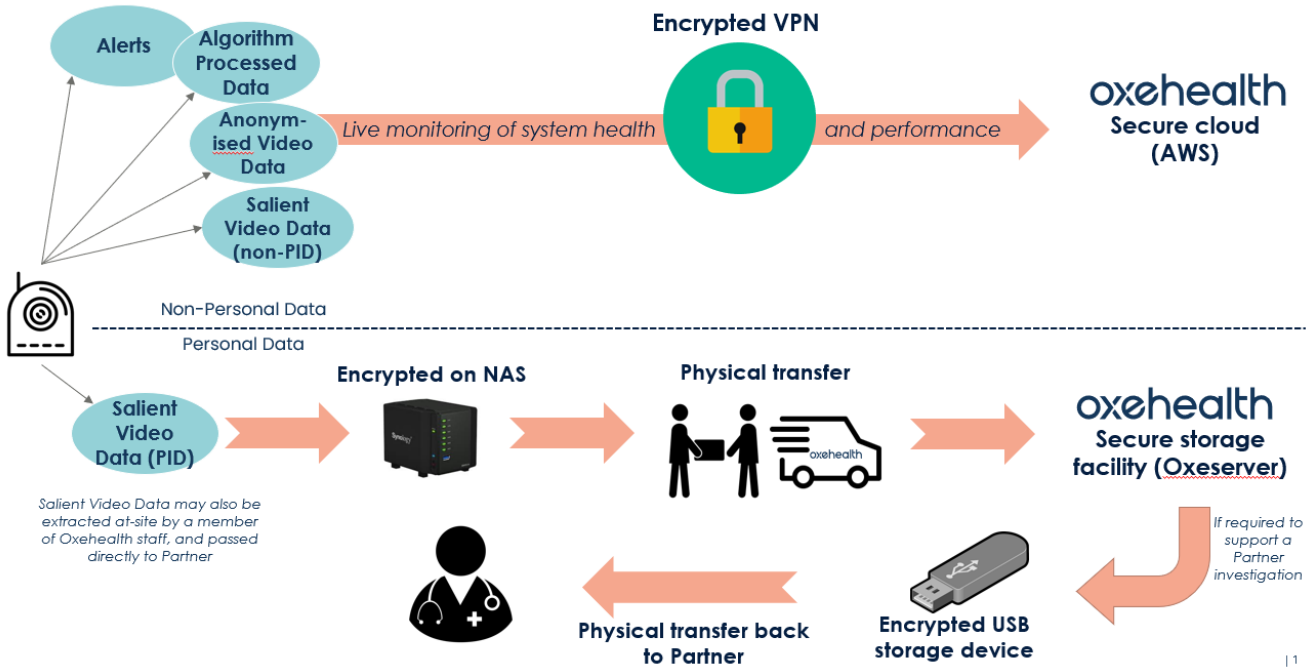
In contrast to Anonymised Video Data, Salient Video Data is encrypted but not anonymised because the identifiable data is required fully to investigate the algorithm's performance (example image, see right). In contrast to Anonymised Video Data, Salient Video Data will be short episodes (typically up 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 securely transferred 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).

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

B. The Data Journey



Data will be collected from every Oxeroom installation and is transferred, in an encrypted format via Ethernet cabling, to the Oxeserver, located in a secure Partner facility.

The Oxehealth Software modules hosted on the 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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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.

If the data has been extracted to support a Partner investigation (ie purpose (4) above), the Salient Video Data clip will be transferred to an encrypted USB storage device and securely transported back to Partner by Oxehealth staff (or a delegated secure courier) in a format that allows it to be extracted securely by Partner staff.

c) Data that is passed directly to Partner without leaving site

Further to the process outlined under (b) above, if Partner requests a clip of Salient Video Data to support an investigation, Oxehealth may alternatively deliver this by a member of Oxehealth staff traveling to the Partner site, extracting the Salient Video Data clip from the Oxeserver onto an encrypted USB stick and passing it directly to the appropriate member of Partner staff.

C. Usage of Data at Oxehealth

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 transferred to Oxehealth's facilities from time to time. Data may be clipped for the following purposes.

1. Oxehealth may clip empty room Salient Video Data 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 Video Data and Algorithm Processed Data.

2. Within three (3) months of installation, Oxehealth may clip an average of up to [60] mins of Personally Identifiable Salient Video Data per room, and no more than [120] minutes for any individual room, which it will select automatically using algorithmic methods. Oxehealth will retain this data for the purpose of validating and testing current and future functionality as the software is updated over time. This is to ensure that the Oxehealth System is continuously optimised for all Partner rooms where the Oxehealth System is live, and to avoid potential performance issues affecting the Oxehealth System.

3. Oxehealth may clip Personally Identifiable Salient Video Data for the purpose of investigating a potential performance issue affecting the Oxehealth System which has been flagged by either Oxehealth Personnel or Partner Personnel. Oxehealth may clip and review short periods of Salient Video Data (including Personally Identifiable Salient Video Data) to understand why certain system outputs are being generated or are failing to be generated, to investigate and resolve any technical issues affecting the Oxehealth Service and to improve the Oxehealth Service for the purpose of providing the Oxehealth Service to the Partner.

4. Oxehealth may clip Salient Video Data at the request of Partner Personnel flagging the need to store the Salient Video Data to support an internal or external investigation, or to provide insight into an event of interest to them

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.

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.

D. Storage and Retention

Non-Personal Data

The Anonymised Video Data, User Interface Output Data and Algorithm Processed Data are stored in Oxehealth's secure remote hosting facility, provided by Amazon Web Services. This hosting is located physically in the UK for UK-based customers, and in Sweden for customers in Sweden or other EU countries. This data is retained for up to two years before it is deleted.

Personal Data

The Personally Identifiable Salient Video Data will generally only be kept for as long as is needed to answer queries raised by NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST staff or by engineers at Oxehealth. To support this, all data files are date and time stamped so that retention can be tracked. However, with respect to Personally Identifiable Salient Video Data collected under purposes (2) and (3) above, Oxehealth may retain the data for up to two years from the date it is extracted, or until the end of the project, or when no longer needed, whichever is earlier. The purpose of retaining data even once a specific Partner query or performance issue has been resolved, is to enable validation and testing of future updates or releases of the Oxehealth System for Partner, to enable the delivery of the Oxehealth Service to the Partner to the contracted SLA.

If collected under purpose (2) above, Oxehealth may, at its own discretion, clip up to a further 60 minutes of Personally Identifiable Salient Video Data per room on average (and no more than 120 minutes for any individual room) to replace data that was deleted within the initial two year retention period, and may continue to do so in cycles of no more than two years for the duration of the Term. Oxehealth may opt to retain data for longer than two years in exceptional circumstances, for example where there is an unusual phenomenon observed in a room which is deemed important to retain for regression testing. In the case of retention for more than two years, Oxehealth will clearly flag this in the regular reporting provided to Partner.

Data collected under purpose (4) above is not retained by Oxehealth, but provided directly to the Partner to support their investigation.

At least twice per year, Oxehealth provides its Partner with a Salient Video Data Report which details the volume, retention period and retention purpose for any Personally Identifiable Salient Video Data collected for the Partner. Oxehealth will process all personal data generated in the project in accordance with this DPIA and

documented instructions from NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST, the Data Controller.

Salient Video Data will be securely deleted at the end of the project, after the two year retention period, or when no longer required, whichever is the earlier. In addition, NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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.

E. Data Ownership

Data ownership is laid out in the Oxehealth Services Agreement.

The Partner 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.

F. Data Security

Oxehealth has implemented an Information Security Management System (ISMS) for assessing and managing security technology and policies to ensure measured protection of all assets (including Partner information assets). Amongst the many controls in place, Oxehealth's storage servers are within a secure 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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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.

G. NHS Data Standards

Oxehealth is ISO13485 and ISO27001 certified, and Oxehealth holds the UK Government Cyber Essentials 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.

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 video data could become public. A breach of the patient's privacy and confidentiality, if information about their treatment is made known to third parties. This could cause distress to the patients.
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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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	Data moved to another country with different data protection rules	GDPR Article 45	Reduced protection on rights and freedoms of data subjects.

In addition to the risks to the individual, any non-compliance could lead to regulatory action, reputational damage, or loss of public trust in NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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

NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST already have strict practices surrounding data confidentiality and privacy of patients, governed by the NHS Code of Confidentiality and the Caldicott Principles. No additional personal data will be made available to NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST staff as a result of this project.

The Oxeserver will be located securely at NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST with physical and electronic access restricted to authorised NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST or Oxehealth personnel. NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST staff are bound

contractually by the Caldicott Principles and the NHS Code of Confidentiality. In addition, the video data held on an Oxeserver is in a proprietary format which could not be viewed with publicly available software. The risk of data being disclosed or lost by a member of NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST staff is therefore deemed to be very low.

To avoid a potential data leak due to theft or malicious electronic attack (and therefore mitigate the risk of accidental damage to or loss of data), Oxehealth have a number of preventative measures in place, including:

- A detailed code of conduct for Oxehealth staff surrounding the use and security of patient data – this clearly states that data should not be used for publicity, information about patients should not be discussed outside of the office and no data should be copied off company servers
- The Oxeserver, and the data contained therein, is held within a secure area at NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST
- Portable storage devices are always accompanied in transit by Oxehealth staff or a secure courier
- Salient Video Data storage is in a secure room with limited keyholder access in a building with 24-hour security guards. This is backed up at Oxehealth, until secure deletion.
- Oxehealth's network is protected with a perimeter UTM firewall, scanning and protecting the gateway from external threats (including intrusion prevention, anti-virus, anti-spyware and botnets)
- Network storage and fileservers are only accessible from the Oxehealth IP range, using individual logons only
- All data collected and generated by the Oxehealth system is anonymised and therefore not personally identifiable. The only exception to this is Salient Video Data (which includes raw video data and is needed to ensure the service is delivered to the contracted standard). In addition to the above measures, to manage any further potential risk from Salient Video Data:
    - The data is securely encrypted
    - It is held separately from the Anonymised Video Data and Algorithm Processed Data
    - Access to Salient Video Data requires authorisation by a member of Oxehealth Senior Management

Risk 2 – Unnecessary intrusion into a patient's privacy

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

As discussed above, all data collected and generated by the Oxehealth system is anonymised and therefore not personal data. The only exception to this is Salient Video Data (which includes raw video data and is needed to ensure the service is delivered to the contracted standard). The use of Salient Video Data is kept to a minimum, used only when NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST want to bring something to the attention of Oxehealth in order to ensure the Oxehealth Service delivers the Contract Purpose to the contracted standard or flag the need to store data to support an internal or external investigation or Oxehealth's engineers flag data that they believe should be reviewed to ensure the Oxehealth Service delivers the Contract Purpose to the contracted standard.). At no point do Oxehealth staff have access to patient names, medical history or reason for being in the hospital.

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

All data collected and generated by the Oxehealth system is anonymised and therefore not personal data, with the exception of the Personally Identifiable Salient Video Data (which is only used minimally as explained above).

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

In the event of a member of the Oxehealth team being able to identify a patient involved in the project, Oxehealth will consult Partner; the default action is to delete all data relating to that patient but Partner 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, NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST (unless applicable law prevents Oxehealth from doing so).

All data collected and generated by the Oxehealth system is anonymised and therefore not personal data.

The exception to this is Personally Identifiable Salient Video Data (which is only used minimally as explained above in Risk 2). The Personally Identifiable Salient Video Data will only be kept for as long as is needed to answer queries raised by NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST staff or by engineers at Oxehealth.

To support this, all data files are date and time stamped so that retention can be tracked, reviews of data stored are undertaken regularly. 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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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, NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST have the ability to request that Oxehealth delete Personally Identifiable Salient Video Data at any time.

Risk 5 – Patient is unaware their data is being collected

Patients in the proposed rooms of NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST are in the care of expert and highly trained NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST staff who will take decisions in the best interest of those patients. NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST will maintain a regime that informs patients in an appropriate fashion.

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

As explained above, only minimal personally identifiable data (Salient Video Data) will be retained as part of the project and this will only be retained for the minimum time necessary.

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

6. DPIA Outcomes

The Partnership being proposed between Oxehealth and NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST is to ensure respect for the patient and their privacy at all times and that any data generated during the project is processed, transferred, stored or reviewed in a safe and timely manner that complies with Data Protection legislation and the Caldicott Principles.

A thorough assessment of the potential risks which might impact a patient's privacy has been undertaken 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.

Recommended by: Date: 15/10/2021

Tom Hatfield
COO and DPO, Oxehealth Limited

DPIA Approval: 

Date: 15/10/2021

Hugh Lloyd-Jukes
CEO, Oxehealth Limited

Appendix 1

Optional Data Protection Officer sign off form.

The Oxehealth Services Agreement requires that the Partner 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 (3) 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 NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS 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.

Signed …*E M Griffiths*

Name: …ELIZABETH GRIFFITHS……

Data Protection Officer for and on behalf of
NORTH STAFFORDSHIRE COMBINED HEALTHCARE NHS TRUST

Date: 18/10/2021

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

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

Data should be collected for specified and explicit purposes and not be used in a way someone wouldn't expect – The purpose for which the Oxehealth system is being used by a Partner 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. All data collected and processed as part of this project is anonymised and non-personally identifiable. The only exception is Salient Video Data which is needed to fully debug the system or enable additional investigations to improve project functionality. The use of Salient Video Data is kept to a minimum, used only when Partner wants to bring something to the attention of Oxehealth in order to improve functionality or Oxehealth's engineers identify sections requiring analysis. At no point do Oxehealth staff have access to patient names, medical history or reason for being in the room.

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

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

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');**

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

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');**

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

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

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').**