

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

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

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

DPIAs are mandatory in certain circumstances, such as when using the health and care data of a large number of people. However, health and care organisations are strongly advised to complete a DPIA when using and sharing personal data in a new way or where there is a substantial change.

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

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

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

This template is written so that it is easy to use without needing expertise in data protection.

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

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

| | |
|---|--------------------------------|
| Data Protection Impact Assessment (DPIA) Title | Oxehealth - Oxevision Software |
| Project Lead | [REDACTED] |
| Contact Details | [REDACTED] |
| DPIA Reference Number | DPIA037 |

SECTION 1 - DO YOU NEED TO DO A DPIA?

| | |
|--|--|
| 1 | Do you need to do a DPIA? |
| <p>Oxehealth is a spin-out from Oxford University which develops proprietary software that support clinical staff in caring for the safety and health of their patients.</p> <p>Oxevision is a contactless patient monitoring platform for mental health. It consists of camera-based hardware and a suite of software modules including two medical devices. Oxevision improves clinicians' ability to observe patients, intervene when necessary and plan care effectively.</p> <p>Kent and Medway NHS and Social Care Partnership Trust procured the following modules for use in two seclusion rooms within the Extra Care Areas in Littlebrook Hospital, Dartford –</p> <ul style="list-style-type: none"> • Oxehealth Vital Signs – spot check measurements of pulse and breathing rate. • Activity Detention – real-time alerts when no activity/movement is detected in an occupied room. <p>Oxevision uses a secure optical sensor which includes a digital camera to monitor the patient's movements. It uses this information to know where the patient is in the room and notifies staff when you may need help. It does not monitor the patient in the bathroom – it only knows they have entered it. The optical sensor is also used to take contact-free pulse rate and breathing rate observations. The installation of Oxehealth does not change current ward operational polices and will not be used as the sole basis for making clinical decisions or recommendations.</p> <p>A DPIA is required as this is new technology and the data that the Trust are collecting is sensitive as relates to health and care.</p> | |
| 1a | Summary of how data will be used and shared |
| <p>Data will be collected via the software directly from the patient, only when still, and will measure a patient's pulse and respiration. Almost all data collected and processed is processed is anonymised and non-personally identifiable (either because the video data is anonymised through techniques such as blurring or because the data is of a mathematical or algorithmic nature).</p> | |

The only exception to this is Salient Video Data. The Oxehealth Software enables partner personnel to be able to tag time periods during which events of interest to them have occurred and for which they would like to be briefed on the algorithm's performance and potential or which contain an Incident that they wish to review.

Various data (anonymised video data, algorithm processed data, alert data and partner input data) will be shared with Oxehealth via the Internet (via encrypted connection) this is shared to improve the system. None of this data is personal data.

| | | |
|-----------|------------------------------------|--|
| 1b | Project Intended Outcome | |
| | Put an [x] next to all that apply. | |
| | X | Personal data – individuals can be identified |
| | | Pseudonymised data - identifiers, for example name or NHS number, are replaced with a unique number or code (a pseudonym) |
| | X | Anonymous data - not identifiable, for example trends or statistics |

SECTION 2 - WHY DO YOU NEED THE DATA?

| | |
|--|---|
| 2 | What are the purposes for using or sharing the data? |
| <p>The purpose of using the Oxevision software is to complete spot check measurements of pulse and breathing rate and provide KMPT with real-time alerts when no activity/movement is detected in an occupied room.</p> <p>Various data (anonymised video data, algorithm processed data, alert data and partner input data) will be shared with Oxehealth via the Internet (via encrypted connection) this is shared to improve the system and to deliver the service to the contracted standard.</p> | |
| 3 | What are the benefits of using or sharing the data? |
| <p>The benefits of using the Oxevision software is to enhance patient and staff safety and patient experience within the two seclusion rooms for use when a patient's acute mental health presentation may mean it is unsafe to enter the patient's room and also in particular for night time monitoring patients to assist with their sleep pattern during regular night time checks.</p> <p>Various data (anonymised video data, algorithm processed data, alert data and partner input data) will be shared with Oxehealth via the Internet (via encrypted connection) this is shared to improve the system and to deliver the service to the contracted standard.</p> | |

SECTION 3 - WHAT DATA DO YOU WANT TO USE OR SHARE?

| | |
|----------|---|
| 4 | Can you use anonymous data for your purposes? If not, explain why. Put an [x] next to the one that applies. |
|----------|---|

| | | |
|----------|---|---|
| | X | Yes |
| | | No |
| | | Unsure – try to provide an explanation of what you think |
| 5 | Which types of personal data do you need to use and why? Put an [x] next to all that apply. | |
| X | Forename | Physical description for example height |
| X | Surname | Phone number |
| | Address | X Email address |
| | Postcode – full | GP details |
| | Postcode – partial | X Legal representative name (personal representative) |
| | Date of birth | X NHS Number |
| | Age | |
| | Gender | |

A patient will be identifiable within a seclusion room by KMPT staff only who will need to make use of a patients NHS Number of Rio ID to access their electronic patient record and record observations and alerts recorded by the Oxevision software.

Salient video footage requested for the purposes of an investigation will be identifiable (not blurred).

Staff data shared with Oxehealth includes forename, surname and NHS email address.

| | | |
|----------|---|---|
| 6 | Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Which types of special category data do you need to use or share? Put an [x] next to all that apply. | |
| | Type of data | Reason why this is needed (leave blank if not applicable) |
| X | Information relating to an individual's physical or mental health or condition, for example information from health and care records | KMPT provides the mental health care and treatment for the Kent and Medway area therefore this data will be processed naturally by the Trust. |
| | Biometric information in order to uniquely identify an individual, for example facial recognition | |
| | Genetic data, for example details about a DNA sample taken as part of a genetic clinical service | |
| | Information relating to an individual's sexual life or sexual orientation | |

| | | |
|----------|--|--|
| X | Racial or ethnic origin | KMPT provides the mental health care and treatment for the Kent and Medway area therefore this data will be processed naturally by the Trust. As the Oxevision software also includes the recording of video this data may naturally be captured within the footage. |
| | Political opinions | |
| | Religious or philosophical beliefs | |
| | Trade union membership | |
| | None of the above | |
| 7 | Who are the individuals that can be identified from the data? Put an [x] next to all that apply. | |
| X | Patients or service users | |
| X | Staff | |
| | Wider workforce | |
| | Visitors | |
| | Members of the public | |
| | Other | |
| 8 | Where will your data come from? Data will be collected directly from patients and staff. | |
| 9 | Will you be linking any data together? Put an [x] next to the one that applies. | |
| | Yes – provide an explanation below and then go to 9a | |
| X | No – skip to question 10 | |
| | Unsure – try to provide an explanation of what you think then go to question 9a. | |

SECTION 4 - WHERE WILL DATA FLOW?

| | | | | | | | | |
|---------------------------------------|---|--|---------------------------------------|--------------------------|--------------------------|-------------------------|--------------------------|--|
| 10 | Describe the flows of data | | | | | | | |
| | | | | | | | | |
| 11 | <p>Confirm that your organisation's information asset register (IAR) or record of processing activities (ROPA) has been updated with the flows described above.</p> <p>Put an [x] next to the one that applies.</p> <table border="1"> <tr> <td><input checked="" type="checkbox"/> X</td> <td>Yes</td> </tr> <tr> <td><input type="checkbox"/></td> <td>No</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Unsure – add as a risk in section 10 with an action to find out</td> </tr> </table> | | <input checked="" type="checkbox"/> X | Yes | <input type="checkbox"/> | No | <input type="checkbox"/> | Unsure – add as a risk in section 10 with an action to find out |
| <input checked="" type="checkbox"/> X | Yes | | | | | | | |
| <input type="checkbox"/> | No | | | | | | | |
| <input type="checkbox"/> | Unsure – add as a risk in section 10 with an action to find out | | | | | | | |
| 12 | <p>Will any data be shared outside of the UK?</p> <table border="1"> <tr> <td><input checked="" type="checkbox"/> X</td> <td>Yes – go to question 12a</td> </tr> <tr> <td><input type="checkbox"/></td> <td>No- skip to question 13</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Unsure – add as a risk in section 10 with an action to find out then skip to question 13</td> </tr> </table> | | <input checked="" type="checkbox"/> X | Yes – go to question 12a | <input type="checkbox"/> | No- skip to question 13 | <input type="checkbox"/> | Unsure – add as a risk in section 10 with an action to find out then skip to question 13 |
| <input checked="" type="checkbox"/> X | Yes – go to question 12a | | | | | | | |
| <input type="checkbox"/> | No- skip to question 13 | | | | | | | |
| <input type="checkbox"/> | Unsure – add as a risk in section 10 with an action to find out then skip to question 13 | | | | | | | |
| a | <p>If yes, give details, including any safeguards or measures put in place to protect the data whilst outside of the UK.</p> <p>Staff identification data (for the receipt of reports created by Oxehealth software) will be processed in the USA. This will be limited to forename, surname and NHS email address.</p> | | | | | | | |

SECTION 5 - IS THE INTENDED USE OF THE DATA LAWFUL?


| | | |
|----|--|--|
| 13 | <p>Under UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?</p> <p>Put an [x] next to the one that applies.</p> | |
| a | <input checked="" type="checkbox"/> | <p>We have consent - This must be 'freely given, specific, informed and unambiguous. You should not rely on this for individual care or research, but is likely to be needed for the use of cookies on a website.</p> |

| | | | |
|-----------|--|----------|--|
| | b | | We have a contractual obligation - between a person and a service, such as a service user and privately funded care home. |
| | c | | We have a legal obligation - the law requires us to do this, for example where NHS Digital or the courts use their powers to require the data. See Annex 2 for the most likely laws that apply when using and sharing information in health and care. |
| | e | x | We need it to perform a public task - a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities. See Annex 2 for the most likely laws that apply when using and sharing information in health and care. |
| | f | | We have a legitimate interest - for example, a private care provider making attempts to resolve an outstanding debt for one of its service users. |
| | | | Other |
| 14 | If you have indicated in question 6 that you are using special category data, what is your lawful basis under UK GDPR? The list below contains the most likely conditions applicable to health and care services. Put an [x] next to the one that applies. | | |
| | b | | We need it to comply with our legal obligations for employment - for example, to check a person's eligibility to work in the NHS or a local authority. See Annex 2 for the most likely laws that apply when using and sharing information in health and care. |
| | f | | We need it for a legal claims or judicial acts - the information is required to exercise, enforce or defend a legal right or claim, for example a person bringing litigation against a health or care organisation. |
| | g | | We need to comply with our legal obligations to provide information where there is a <u>substantial public interest</u>, with a basis in law - for example, setting up a system to share safeguarding information. See Annex 2 for the most likely laws that apply when using and sharing information in health and care. |
| | h | x | We need it to comply with our legal obligations to provide or manage health or social care services - providing health and care to a person, or ensuring health and care systems function to enable care to be provided. See Annex 2 for the most likely laws that apply when using and sharing information in health and care. DPA18 Schedule 1 Part 1 Section 2 |
| | i | | We need it to comply with our legal obligations for public health - using and sharing information is necessary to deal with threats to public health, or to take action in response to a public health emergency (such as a vaccination programme). See Annex 2 for the most likely laws that apply when using and sharing information in health and care. |
| | j | | We need it for archiving, research and statistics where this is in the public interest - for example, a clinical trial for a new drug, with relevant safeguards in place for the use of the participant's health and care information. See Annex 2 for the most likely laws that apply when using and sharing information in health and care. |
| | | | Other |
| | | | Not applicable - the use of special category data is not proposed |
| 15 | What is your legal basis for processing health and care data under the common law duty of confidentiality? Put an [x] next to the one that applies. | | |
| | | | <u>Implied consent</u> - for individual care or local clinical or care audits - skip to question 16. |

| | | |
|--|---|---|
| | | Explicit consent - a very clear and specific statement of consent - go to question 15a. |
| | | Section 251 support - this means you have approval from the Secretary of State for Health and Care or the Health Research Authority following an application to the Confidentiality Advisory Group (CAG). CAG must be satisfied that it isn't possible or practical to seek consent. Go to question 15a. |
| | X | Legal requirement - this includes where NHS Digital has directed an organisation to share the data using its legal powers. State the legal requirement in the further information section. Go to question 15a. |
| | | Substantial public interest - for example to prevent or detect a serious crime or to prevent serious harm to another person. The justification to disclose must be balanced against the public interest in maintaining public confidence in health and care services. An example would be setting up a system to notify relevant organisations of safeguarding concerns. Go to question 15a. |
| | | Not applicable - we are not proposing to use health and care data. Skip to question 16. |
| Provide evidence as follows depending on your selection in question 15: | | |
| Health and Social Care Act 2012 | | |

SECTION 6 - HOW ARE YOU KEEPING THE DATA SECURE?

| | | |
|--|--|---|
| 16 | Are you collecting information? Put an [x] next to the one that applies. | |
| | X | Yes – go to question 16a |
| | | No – skip to question 17 |
| 17 | Are you storing information? Put an [x] next to the one that applies. | |
| | X | Yes – go to question 17a |
| | | No – skip to question 18 |
| a | How will information be stored? Put an [x] next to all that apply. | |
| | | Physical storage, for example filing cabinets, archive rooms etc |
| | | Local organisation servers – Oxeserver within secure Server Room with additional NAS for Salient Video Data |
| | | Cloud storage – Oxehealth Secure Cloud Services |
| | | Other |
| 18 | Are you transferring information? Put an [x] next to the one that applies. | |
| | X | Yes - go to question 18a |
| | | No - skip to question 19 |
| a | How will information be transferred? | |
| <p>Personally, identifiable data will be encrypted at rest to the AES256 standard or equivalent the local secure servers and/or NAS at customer site.</p> <p>All data transmission between local computer equipment at customer site will take place over a secure virtual private network (VPN) which ensures communication between authenticated device only, using encryption to AES256 standard or equivalent.</p> | | |



| | |
|--|---|
| Any data transfers over the internet will use SSL encryption to the AES256 standard. | |
| 19 | How will you ensure that information is safe and secure? Put an [x] next to all that apply. |
| | <input checked="" type="checkbox"/> Encryption – SSL/AES 256 |
| | <input type="checkbox"/> Password protection – For computer devices. |
| | <input type="checkbox"/> Role based access controls (RBAC) – for access to electronic patient record where data will be recorded. |
| | <input checked="" type="checkbox"/> Restricted physical access – for access to server room on KMPT site. |
| | <input type="checkbox"/> Business continuity plans |
| | <input checked="" type="checkbox"/> Security policies  OxehealthSOPKMPT .CliG.245.01.pdf |
| <input type="checkbox"/> Other | |
| | |
| 20 | How will you ensure the information will not be used for any other purposes beyond those set out in question 2? Specify the measures below which will be used to limit the purposes the data is used for. Put an [x] next to all that apply and provide details. |
| | <input checked="" type="checkbox"/> Contract |
| | <input type="checkbox"/> Data processing agreement |
| | <input type="checkbox"/> Data sharing agreement |
| | <input type="checkbox"/> Audit |
| | <input checked="" type="checkbox"/> Staff training |
| | <input type="checkbox"/> Other |


SECTION 7 - HOW LONG ARE YOU KEEPING THE DATA AND WHAT WILL HAPPEN TO IT AFTER THAT TIME?

| | |
|---|--|
| 21 | How long are you planning to use the data for? |
| We intend to process anonymous data via this platform for duration of the contract. | |
| 22 | How long do you intend to keep the data? |
| Clear video Data (CVD) is stored for 24hrs and then automatically deleted by the software. Patient health record data (PHRD) is stored for 7 days and then automatically deleted by the software. Staff identification data (SID) will be stored until the end of the contract. | |
| 23 | What will happen to the data at the end of this period? Put an [x] next to all that apply. |

| | | |
|--|---|---|
| | X | Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction) |
| | | Permanent preservation by transferring the data to a Place of Deposit run by the National Archives |
| | | Transfer to another organisation |
| | | Extension to retention period – with approved justification |
| | | It will be anonymised and kept |
| | | Other |

SECTION 8 - HOW ARE PEOPLE'S RIGHTS AND CHOICES BEING MET?

| | | |
|--|--|--|
| 24 | How will you comply with the following data subject rights (where they apply)? | |
| Individual Right | | How will you comply (or state <i>not applicable</i> if the right does not apply) |
| The Right to be Informed The right to be informed about the collection and use of personal data. | | We have assessed how we should inform individuals about the use of data for Oxehealth – Oxevision . We consider the communications methods below meet this obligation. Put an [x] next to all that apply. |
| | | X Privacy notice(s) for all relevant organisations pn020-oxehealth.pdf |
| | | X Information Leaflets  Oxehealth Leaflet. 2.3.pdf |
| | | X Posters  OxehealthSOPKMPT .CliG.245.01.pdf |
| | | Letters |
| | | Emails |
| | | Texts |
| | | Social media campaign |
| | | X DPIA Published |
| | | Other |
| | Not applicable | |
| The right of access The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request. | | KMPT Access to healthcare records |
| The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete. | | Individuals are able to exercise their right to rectification by making a request to the Information Governance & Records Management Department |
| The right to erasure | | This right does not apply. |


| | | |
|---|--|---|
| The right to have personal data erased. | | |
| The right to restrict processing The right to limit how their data is used. | | Individuals are able to exercise their right to restrict processing by making a request to the Information Governance & Records Management Department. |
| The right to data portability The right to obtain and re-use their personal data. | | Individuals are able to exercise their right to data portability by making a request to the Information Governance & Records Management Department. |
| The right to object The right to object to the use and sharing of personal data. | | Individuals have a right to object to their data being shared with Oxehealth. If an individual object this will initially be reviewed as per –  OxehealthSOPKMPT .CliG.245.01.pdf |
| 25 | Will the national data opt-out need to be applied? Put an [x] next to the one that applies. | |
| | | Yes |
| | X | No |
| | | Unsure – add as a risk in section 10 with an action to find out |
| 26 | Will any decisions be made in a purely automated way without any human involvement (automated decision making)? Put an [x] next to the one that applies. | |
| | | Yes - go to question 26a |
| | X | No - skip to question 27 |
| | | Unsure – add as a risk in section 10 with an action to find out |
| 27 | Detail any stakeholder consultation that has taken place (if applicable). | |
| N/A | | |


SECTION 9 - WHICH ORGANISATIONS ARE INVOLVED?

| | |
|--|--|
| 28 | List the organisation(s) that will decide why and how the data is being used and shared (controllers). |
| Kent and Medway NHS and Social Care Partnership Trust | |
| 29 | List the organisation(s) that are being instructed to use or share the data (processors). |
| Oxehealth | |
| 30 | List any organisations that have been subcontracted by your processor to handle data |
| Gitlab (USA), Snowflake (Cloud Server), AWS data centres (EU)& Egress (EU) | |
| 31 | Explain the relationship between the organisations set out in questions 28, 29 and 30 and what activities they do |

| | | |
|--|---|---|
| Gitlab (USA server) – staff data (first name, surname and NHSmail address) Snowflake (Cloud Server) – encrypted digital observation data AWS data centres (EU Cloud Storage) – encrypted digital observation data Egress (EU) – transfer of observation reports to clinical staff | | |
| 32 | What due diligence measures and checks have been carried out on any processors used? Put an [x] next to all that apply. | |
| | X | Data Security and Protection Toolkit (DSPT) compliance Oxehealth - Organisation Details |
| | X | Registered with the Information Commissioner's Office (ICO) Oxehealth - Information Commissioner's Office - Register of data protection fee payers - Entry details AWS - Information Commissioner's Office - Register of data protection fee payers - Entry details Egress - Information Commissioner's Office - Register of data protection fee payers - Entry details |
| | | Digital Technology Assessment Criteria (DTAC) assessment |
| | X | Stated accreditations Oxehealth – ISO13485, ISO27001 & DCB0129 |
| | | Data security or Cyber Essentials certification Oxehealth - BM Registry aa1c77bf-a477-4f6f-8875-a8cfd696951c |
| | | Other checks |

SECTION 10 - WHAT DATA PROTECTION RISKS ARE THERE AND WHAT MITIGATIONS WILL YOU PUT IN PLACE?

| 33 | Complete the risk assessment table. Use the *risk scoring table to decide on the risk score. | | | |
|-----------------------|--|---------------------|---|--------------------------------------|
| Risk Assessment Table | | | | |
| Risk Reference Number | Description | Risk Score* (L x I) | Mitigations | Risk Score* with mitigations applied |
| 01 | The video data could become public, leading to a breach of the patient’s privacy and dignity. This could cause distress to the patients. | 12 | Data is in a proprietary format which cannot be viewed on publicly available software and there are physical and technical security measures in place to protect the data from theft or malicious attack. | 2 |
| 02 | 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. | 12 | The system is not a CCTV monitoring system - there is no continuous feed of video data to clinician. Clear Video Data usage is limited and for very specific defined purposes as outlined in the Trusts SOP.  OxehealthSOPKMPT .CliG.245.01.pdf Oxehealth staff do not have access to view the video data on the system. | 2 |
| 03 | An Oxehealth staff member identifies a patient known to them personally when working with CVD and tells other people known to the patient. This could cause distress to the patients. | 2 | Oxehealth does not transfer or store CVD outside of the secure servers located on customer site, other than to provide it to customers as part of a Serious Incident review. Oxehealth have implemented policies | 2 |

| | | | | |
|----|--|---|--|---|
| | | | and procedures to ensure the data is not viewed by Oxehealth staff in the process of transferring it | |
| 04 | Personally Identifiable Patient data is retained for longer than necessary, increasing the security risk and risk of breach of confidentiality | 6 | Data is only kept for as long as required to fulfil the purpose. All data files are time stamped so retention can be tracked and reviews of data are undertaken regularly. | 2 |
| 05 | Patient unaware their data is being collected and are unable to exercise their rights under GDPR. | 9 | <p>There is national guidance including patient information leaflets and posters for customers to use with patients to inform them of the system.</p> <p>Oxehealth Resources</p> <p>KMPT also have their own patient leaflet which provides information around the use of Oxevision.</p>  <p>Oxehealth Leaflet. 2.3.pdf</p> | 2 |
| 06 | Personal data is accidentally shared with Oxehealth by customers when requesting support. This could lead to data being processed in Oxehealth systems not designed for personal data storage and processing which increases the security risk and risk of a breach of confidentiality | 9 | <p>Oxehealth provides on-screen warnings to staff to avoid personal data on all Oxehealth software functions where data may accidentally be shared, staff are trained on the use of software as part of the service.</p> <p>Oxehealth have implemented a redaction and deletion process to ensure any personal data accidentally shared is removed from all Oxehealth records and not further processed by Oxehealth staff.</p> | 2 |
| 07 | Data is moved to another country with different data protection rules leading to a reduced protection on rights and freedoms of data subjects. | 9 | <p>Oxehealth will ensure any data transfer outside the customer location meets with relevant privacy regulations and contracts with sub-processors include appropriate safeguarding measures for data transfer</p> <p>Oxehealth will notify customers of any changes to sub-</p> | 2 |

| | | | | |
|--|--|--|--|--|
| | | | processors and data transferred as required in the service agreement signed with them. | |
|--|--|--|--|--|

| | | LIKELIHOOD | | | | |
|--------|-------------------|------------|---------------|---------------|-------------|------------------------|
| | | 1 Rare | 2 Unlikely | 3 Possible | 4 Likely | 5 Almost Certain |
| IMPACT | 5 Catastrophic | 5 | 10 | 15 | 20 | 25 |
| | 4 Major | 4 | 8 | 12 | 16 | 20 |
| | 3 Moderate | 3 | 6 | 9 | 12 | 15 |
| | 2 Low | 2 | 4 | 6 | 8 | 10 |
| | 1 Negligible | 1 | 2 | 3 | 4 | 5 |

SECTION 11 - REVIEW AND SIGN OFF

| | |
|-----------------------------------|--|
| IG Lead | |
| Name | |
| Date | |
| Signature | |
| Data Protection Officer | |
| Name | |
| Date | |
| Signature | |
| Caldicott Guardian | |
| Name | |
| Date | |
| Signature | |
| SIRO | |
| Comment/consideration and advice: | |
| Name | |
| Date | |
| Signature | |

Appendix A

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

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

Abortion Act 1967 and Abortion Regulations 1991

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

Access to Health Records Act 1990

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

Care Act 2014

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

Children Act 1989

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

Control of Patient Information Regulations 2002 (COPI)

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

Coroners and Justice Act 2009

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

Employment Rights Act 1996

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

Equality Act 2010

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

Female Genital Mutilation Act 2003

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

Fraud Act 2006

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

Health and Social Care Act 2008 and 2012

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

- The Secretary of State for Health and Social Care
- NHS England, which leads the NHS in England
- The Care Quality Commission, which inspects health and care services
- The National Institute for Health and Care Excellence (NICE), which provides national guidance and advice to improve health and care
- NHS Digital, which is the national provider of information, data and IT systems for health and social care.

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

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

Health Protection (Notification) Regulations 2010)

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

Human Fertilisation and Embryology Act 1990

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

Human Tissue Act 2004

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

Inquiries Act 2005

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

Local Government Act 1972

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

NHS Act 2006

Sets out what NHS organisations can and can't do and how they can or can't use information. It allows confidential patient information to be used in specific circumstances for purposes beyond individual care. These

include a limited number of approved research and planning purposes. Information can only be used where it is not possible to use information which doesn't identify you, or where seeking your explicit consent to use the information is not practical. The Act also sets out that information must be shared for the prevention and detection of fraud in the NHS.

Public Records Act 1958

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

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

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

Safeguarding Vulnerable Groups Act 2006

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

Statistics and Registration Service Act 2007

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

Terrorism Act 2000 and Terrorism Prevention and Investigation Measures Act 2011

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

The Road Traffic Act 1988

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

