St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Information Governance Policy and Procedures

Policy Lead	Registered Manager
Version No.	1.2
Date of issue	Mar 2023
Date to be reviewed	Mar 2024
Not controlled once printed	

OXONA HEALTHCARE

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Introduction

Information Governance gives assurance to data subjects, including members of staff, individuals and service users that personal information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care. Oxona Healthcare recognises that it is of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

Policy Statement

All members of staff must comply with this policy. In order to discharge its requirements, Oxona Healthcare ensures that clear policies and procedures are in place and are supported by effective awareness training. Personal data will be:

- obtained, held and processed fairly
- held for specific purposes and used only for these purposes
- processed in accordance with the rights of the data subject
- relevant, accurate and kept up to date
- corrected if shown to be inaccurate
- kept for no longer than necessary and destroyed when no longer required, in line with best practice
- protected against loss or unauthorised or unlawful processing, accidental loss and destruction or damage using appropriate technical or organisational measures.

This policy should be read in conjunction with the Patient Confidentiality Policy.

Oxona Healthcare Data Protection officer is Megan Hickman

Scope

This policy applies to all members of staff at Oxona Healthcare who should ensure that they are aware of their responsibilities in relation to information governance.

This policy applies to all personal data processed by Oxona Healthcare relatable to any identifiable living person.

Definitions

Data subject: The individual about whom Oxona Healthcare has collected personal data.

Data Protection Act 2018: An Act of Parliament that updates data protection laws in the UK. It sits alongside the General Data Protection Regulation and implements the EU's Law Enforcement Directive.

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

General Data Protection Regulation (EU) 2916/679: a regulation in EU law on data protection and privacy for all individuals within the European Union. The relevance of the GDPR is not impacted by UK's departure from the European Union.

Personal data: any information about a living person including, but not limited to, names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data, as defined below.

Process or processing: doing anything with personal data, including, but not limited to, collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data; at the point you collect it, you are processing it.

Special categories of data: has an equivalent meaning to 'sensitive personal data' under the Data Protection Act 2018. Special categories of data include, but are not limited to, medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views.

Data controller: the main decision-maker over the management of the data in question. They exercise overall control over the purposes and means of the processing of personal data. For the purposes of this policy. Oxona Healthcare considers itself to be a data controller in respect of all members of staff and service users.

Data processor: acts on behalf of and only on the instructions of the relevant controller. For the purposes of this policy Oxona Healthcare considers that they are the data processor in relation to the service delivered to its service users.

Personal Data Audits

Oxona Healthcare will carry out PID (Personally Identifiable Data) Audits. The data audit will be carried out by the Data Protection Officer or a person to whom the Data Protection Officer has delegated this task responsibility and the results collated. The personal data audit will identify the following:

- whom the information is held about
- what personal information is held, including any sensitive personal data
- in which format the personal data is being collected (e.g., name, address, telephone number etc.)
- how the PID is stored (e.g., on a computer, manual files or both)
- who has access to this information
- the purpose(s) for which Oxona Healthcare holds the personal data
- how the PID is collected
- whom the PID is collected from.

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

A Personal Data Audit form is available from the Data Protection Officer. The Data Protection Officer will use the outcome of the Personal Data Audit to update the Information Asset Register.

Information Asset Register

Computerised and manual filing systems containing information relating to an identifiable person who can be directly or indirectly identified, such as name, identification number, location data or online identifier, must be documented in the Information Asset Register. The Asset Register will record:

- the Service Area to which the entry relates
- the name of the computer system, manual files or both in which the data is stored
- whom the information is held about
- what personal information is held, including any sensitive personal data that is being held
- how the data is protected (e.g., restricted access or protected access)

Such systems must be managed to comply with GDPR/Data Protection principles.

Access to Information and Disclosure Outside of Oxona Healthcare

Members of staff will be granted access to the information that they need to carry out their work. Members of staff have a duty to keep the information they use confidential.

There are a number of occasions where it will be necessary for Oxona Healthcare to share PID. The correct parameters of when it is appropriate to share and disclose data include relevant agreements and protocols that are in place that allow for the exchange of information between Oxona Healthcare and other organisations. Any information disclosed must be necessary for the purpose for which it is disclosed.

If it is necessary to discuss individual data subjects in reports or at meetings, a pseudonymisation process should be followed (e.g., Nurse A).

Individual Awareness

It is Oxona Healthcare policy that:

- Information Governance (confidentiality) training will be classified as 'mandatory' in the induction programme

St Luke's Hospital
Headington,
Oxford,
OX3 7PF
01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

- all new members of staff to the business will receive information governance training relevant to their role, as soon as possible on commencement of their employment
- all individuals associated with Oxona Healthcare whether employed or contracted, will receive information governance training at least every 3 years or provide certification for similar mandatory training (e.g. from NHS bluestream provider).
- guidance and support is available to all members of staff who process PID.

Security Breach Notification and Investigation

Any breach or suspected breach of the GDPR must be reported immediately to the Data Protection Officer, providing as much information as possible. A breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability or personal data. There will be a personal data breach whenever personal data is lost, destroyed, corrupted or disclosed, as well as if someone accesses the data or passes it on without proper authorisation or if the data is made unavailable, for example when it has been encrypted by ransomware or accidentally lost or destroyed.

The Data Protection Officer will investigate and, if appropriate, produce a report for the Senior Management Team. The Data Protection Officer will provide advice to the Senior Management Team on whether the breach requires notification to the Information Commissioner's Office. This advice should take account of the information provided on the ICO's website regarding the reporting of breaches.

The Data Protection Officer is required to notify the ICO of any breach that is likely to present a risk to the rights and freedoms of data subjects. If a decision is made not to report a breach to the ICO, the rationale must be documented so that it can be justified at a later date if required.

Individual Rights – The Right to be Informed

Oxona Healthcare's privacy notice supplied to members of staff in regards to the processing of their personal data will be written in a clear, plain language, which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- the identity and contact details of Registered Manager and the Data Protection Officer
- the purpose of and the legal basis for processing the data
- the legitimate interest of Oxona Healthcare (if applicable) or a third party

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

- any recipient categories of recipients of the personal data
- any international transfers of data
- how long the data will be stored for
- the existence of the data subject's rights, including the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Individual Rights – Subject Access Requests (SARS)

Individuals have the right to obtain confirmation that their data is being processed. They also have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The GDPR requires that the data subject is provided with access to their personal data within 1 month of their request being validated by Oxona Healthcare. Oxona Healthcare may extend the period of compliance by a further 2 months, where requests are complex or numerous. If this is the case, Oxona Healthcare will inform the individual within 1 month of receipt of the request and explain why the extension is necessary.

Oxona Healthcare will verify the identity of the person making the request before any information is supplied. The Data Protection Officer must be advised of all subject access requests and keep a record of these to demonstrate compliance with the requirements of the legislation. The response time will not commence until all of the conditions identified above been satisfied. All requests will be responded to without delay and at the latest, within 1 month of receipt

A copy of the information will be supplied to the individual free of charge. However, Oxona Healthcare may impose a ''reasonable fee" to comply with requests for further copies of the same information. Fees will be based on the administrative cost of providing this information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will also be charged.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. All manual data in relevant filing systems will be reviewed and any personal data relating to third parties removed, anonymised or consent for its disclosure obtained from the third party.

Where a request is manifestly unfounded or excessive, Oxona Healthcare holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority (the Information Commissioner's Office) within 1 month of the refusal.

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

In the event that a large quantity of information is being processed about an individual, Oxona Healthcare will ask the individual to specify the information the request is in relation to.

Individual Rights – Right to Rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.

Where the personal data in question has been disclosed to third parties, Oxona Healthcare will inform them of the rectification, where possible. Where appropriate, Oxona Healthcare will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within 1 month; this will be extended by 2 months where the request for rectification is complex.

Where no action is being taken in response to a request for rectification, Oxona Healthcare will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

Individual Rights – The Right to Erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances:

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- when the individual withdraws their consent
- when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- the personal data was unlawfully processed
- the personal data is required to be erased in order to comply with a legal obligation
- the personal data is processed in relation to the offer of information society services to a child.

Oxona Healthcare has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

- the exercise or defence of legal claims.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, Oxona Healthcare will inform the other organisations who process the personal data to erase links to and copies of the personal data in question.

Individual Rights – The Right to Restrict Processing

Individuals have the right to block or suppress the processing of personal data used by Oxona Healthcare.

In the event that processing is restricted, Oxona Healthcare will store the personal data, but will not process it further, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. Oxona Healthcare will restrict the processing of personal data in the following circumstances:

- where an individual has objected to the processing and Oxona Healthcare is considering whether there are legitimate grounds to override those of the individual
- where processing is unlawful and the individual opposes erasure and requests restriction instead
- where Oxona Healthcare no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

Where an individual contests the accuracy of the personal data, processing will be restricted until Oxona Healthcare has verified the accuracy of the data. If the personal data in question has been disclosed to third parties, Oxona Healthcare will inform them about the restriction on the processing of the personal data, unless it is impossible or involves a disproportionate effort to do so. Oxona Healthcare will inform individuals when a restriction on processing has been lifted.

Individual Rights – The Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. The right to data portability only applies in the following cases:

- to personal data that an individual has provided to a controller
- where the processing is based on the individual's consent or for the performance of a contract
- when processing is carried out by automated means.

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Personal data will be provided in a structured, commonly used and machine-readable form. The information will be provided free of charge. Oxona Healthcare is not required to adopt or maintain processing systems that are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, Oxona Healthcare will consider whether providing the information would prejudice the rights of any other individual.

Oxona Healthcare will respond to any requests for portability within 1 month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by 2 months, ensuring that the individual is informed of the extension and the reasoning behind it within 1 month of receipt of the request.

Where no action is being taken in response to a request, Oxona Healthcare will, without delay and at the latest within 1 month, explain to the individual the reason for this and will inform them of their right to complain to the Information Commissioner's Office.

Fair and Lawful Processing

Under the GDPR, data will be lawfully processed by Oxona Healthcare under the following conditions:

- the consent of the data subject has been obtained
- processing is necessary for:
    - compliance with a legal obligation
    - the performance of a task carried out in public interest or in the exercise of official authority vested in the controller
    - for the performance of a contract with the data subject or to take steps to enter into a contract
    - protecting the vital interests of a data subject or another person
    - for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Sensitive data will only be processed under the following conditions:

- Oxona Healthcare will not use personal data for any purposes other than those advised to individuals directly or detailed in the relevant entry in the Register of Data Controllers published by the Information Commissioner's Office
- as far as possible, Oxona Healthcare will process personal data only where it is necessary for compliance with the law, the performance of a contract, with a view to establishing a contract, or it is in the organisation's legitimate business interests to do so

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

- where this is not possible, or in the case of sensitive personal data (see below), consent of the individual will be sought to enable the personal data to be processed.

Oxona Healthcare will obtain the explicit consent of the individual concerned for all processing of sensitive personal data, unless:

- it is information relating to racial/ethnic origin, disability or religious belief that is being collected purely for monitoring equality of opportunity or treatment
- it relates to the employment of individuals
- it is necessary for the provision of advice or support and the data subject cannot reasonably be expected to give explicit consent.

Oxona Healthcare will require all data processors to formally agree that personal data will not be used for any purpose other than that agreed. Oxona Healthcare will not disclose personal data to third parties, unless:

- carrying out obligations under employment, social security or social protection law or a collective agreement
- protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- reasons of substantial public interest on the basis of Union or Member State law, which is proportionate to the aim pursued and which contains appropriate safeguards
- the purposes of preventative or occupational medicine, for assessing the working capacity of the members of staff, medical diagnosis, the provision of health, social care, treatment, management of health, or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

All disclosures of personal data to third parties must be authorised by a member of the Senior Management Team and be limited to the minimum information required. All disclosures must be recorded either in the personnel or service user's record.

Retention of Information

OXONA HEALTHCARE

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Personal data shall be retained in accordance with the period detailed below. Where a retention period is not specified, personal information will only be retained for the longer of:

- as long as required for its purpose
- as required by law
- as recommended by the Institute of Personnel Directors.

Paper based records will be disposed of in the confidential waste bins provided ready for shredding. Further advice can be sought from the Data Protection Officer. Oxona Healthcare requires all data processors to formally agree that personal data shall not be retained for longer than the purpose for which they are processing it. In the table below, retention periods in bold are statutory, those not in bold are best practice:

Record	Retention	Comment
Application forms of non-short-listed candidates	**6 months**	Equality Act 2010
Short lists, interview notes and related application forms	6 months	Chartered Institute of Personnel and Development recommendation
Personnel records (incl. training & disciplinary)	6 years after employment ceases	Chartered Institute of Personnel & Development recommendation
Redundancy details/ calculations	6 years after redundancy	Chartered Institute of Personnel & Development recommendation
Wage/salary / payment records	**6 years**	Taxes Management Act 1970
SMP & SSP records (incl. certificates & self-certification)	**3 years after end of related tax year**	SMP Regulations SSP Regulations
Parental leave	5 years from birth/adoption	Chartered Institute of Personnel & Development recommendation
Incident details	10 years after incident	Department of Health NHS Code of Practice for Records Management
RIDDOR incident details	6 years after incident	Limitation Act 1980

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Record	Retention	Comment
Oxona Healthcare members of staff (incl. training / contact information / PID)	6 years after employment ceases	Limitation Act 1980

Methods used for disposal of confidential information must continue to protect confidentiality. Paper information should be shredded by means of the paper shredding service using the secure, locked consoles placed at various sites within Oxona Healthcare.

All redundant, faulty or obsolete removable storage media, such as external hard drives which did or which may have contained sensitive or valuable information during their life cycle, should be returned to the IT team to ensure complete removal of information/information storage capability.

Data Quality

All forms used to collect personal data shall only ask for information that is relevant to the purpose of the form. At least once each year, members of staff and service users will be provided with an opportunity to confirm the accuracy of any personal data held on Oxona Healthcare IT systems.

Changes in personal data relating service users or members of staff must be promptly and accurately updated on the appropriate computer system(s).

All notes recorded will be saved on the personnel file. The information must be accurate and relevant and not express any subjective opinion relating to an individual's personal characteristics.

Disclosing Personal Data

All personal data will be protected from unauthorised access by appropriate organisational and technical security measures. Personal data will not be disclosed to data processors unless there is a contract or confidentiality agreement in place, which defines the authorised use(s) to which the data can be put. Personal data will not be disclosed to the data subject via a telephone or facsimile transmission where the authenticity of the requestor cannot be reliably established.

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Personal data disclosed to the data subject in response to a Subject Access Request must be reviewed before disclosure to ensure that it does not include any information that infringes the rights and freedoms of any third party or is exempt from disclosure.

Personal data will not be disclosed to third parties where the identity of the third party cannot be reliably established. Personal data will only be disclosed to third parties when **one** of the following conditions is met:

- the data subject has given Oxona Healthcare their consent to disclose the information (including where there is a Lasting Power of Attorney)
- disclosure is essential to the lawful purpose for which the personal data is being processed
- the data subject has given the third party their consent to request the information
- the disclosure is subject to a formal Information Sharing Protocol and is made within the terms of that protocol
- disclosure is required by law (including the prevention or detection of crime, apprehension or prosecution of offenders and the assessment or collection of any tax or duty)
- disclosure is in the vital interest of the data subject.

Sensitive personal data will only be disclosed to third parties when **one** of the following conditions is met:

- the data subject has given their explicit consent for the disclosure (including consent by a Lasting Power of Attorney)
- the data subject has given the third party their explicit consent to request the information
- disclosure is required by law (including the prevention or detection of crime, apprehension or prosecution of offenders and the assessment or collection of any tax or duty)
- disclosure is in the vital interest of the data subject.

Disclosure in respect of the last two conditions of this policy must not be made without the formal authorisation of the Data Protection Officer. All disclosures of personal data to data processors and third parties will be limited to the minimum information required to satisfy the requirements of the contract or legitimate request.

Consent must be obtained before an individual's personal data is published in any Oxona Healthcare publication. In the case of sensitive personal data, the consent must be explicit (e.g., signing of the pre-publication article).

The disclosure of personal data must be recorded in an appropriate IT system

Information Security

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Oxona Healthcare has a systematic approach to information security risk management and identifies business needs regarding information security requirements (including contractual and regulatory). During the delivery and maintenance of Oxona Healthcare services, there are a number of instances where risk assessment is necessary (e.g., disclosure to third parties). Risk management shall be completed when it is considered necessary to protect the needs of our people or our information, as follows:

- a practical, clear desk policy will be maintained so that no personal or sensitive information or information of a confidential nature is left on unattended desks or in offices in such a way that it could be accessible to any person who is not authorised to have such access
- information assets and information processing facilities are protected against unauthorised access
- information is protected from unauthorised disclosure
- confidential and sensitive information is appropriately classified as such
- appropriate arrangements are in place to encrypt laptops and emails containing personal information
- appropriate arrangements are in place to manage the uploading and downloading of confidential and sensitive information from IT equipment
- confidentiality of information assets is a high priority
- integrity of information will be maintained
- Oxona Healthcare requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities are met
- statutory, expressed and implied legal obligations are met
- business continuity plans shall be produced, maintained and tested.

Unauthorised and illegal use of information assets and information processing facilities is prohibited. The use of obscene, racist or otherwise offensive statements shall be dealt with in accordance with other policies published by Oxona Healthcare.

This policy is communicated to all individuals working with Oxona Healthcare for whom information governance training shall be given. All breaches of information security, actual or suspected, must be reported and investigated in line with Oxona Healthcare policies. Controls are commensurate with the risks faced by Oxona Healthcare.

White Boards

Any PID should not be displayed in an office on a white board where members of the public can view, or see from the exterior of the building

Computers

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

PID must only be stored on Company equipment and not on personally owned laptops, palm-pilots or home desktop computers.

All files containing personal identifiable information, held on Company owned computer equipment should be "encrypted/password" protected, and preferably not held by the data subject's name, substituting a suitable identifier other than name. Particular care should be taken with portable devices. The ideal is that portable devices should only act as terminals to the main networked system, since the data is then protected in the Company network.

Personal identifiable data should not be kept on the hard drives of PCs unless formally justified by the Data Protection Officer, due to the risk of theft and breach of confidentiality. Such files should be stored on the network, where they will be backed up centrally by the IT team.

Files containing individual person-identifiable information on portable computers should be password protected, or better still not stored on a portable. Files stored on network drives do not require password protecting, as a password is needed to log on to the network and access to folders is restricted.

Users should not leave terminals logged in and unattended. Screens should be locked as soon as the user moves away from the screen to reduce the risk of unauthorised access to information. Computers should not be transferred between users or disposed of, other than through the IT team as they have the means of transferring or removing all data from the hard drive.

Telephones

All possible steps must be taken to ensure that information regarding an individual is not divulged over the telephone to anyone without authority. Asking for key details about the individual (e.g., date of birth) may not be sufficient to ensure that the caller has a need to know.

Where there is any doubt regarding the identity of the person requesting the information, guidance should be sought from the Data Protection Officer. If advice is not immediately available, then the information should not be disclosed. If the caller is claiming to be from an organisation (e.g., the NMC) then the switchboard telephone number should be obtained (rather than direct line), checked and then used to ensure that the caller is from the agency stated.

A record should be kept of all telephone discussions where information is shared verbally on the personnel file.

Email

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Personal email addresses should never be used for work purposes. Person identifiable information must only be sent by e-mail within Oxona Healthcare when attached to a password protected document, spreadsheet or database. Inclusion within the main body of the e-mail is not permitted. Notes are transmitted to patients only as attachments. The password is be delivered to the recipient by a different medium, such as a telephone call or text message

Personal identifiable information must only be sent externally using an encrypted email. Steps must be taken to ensure that any confidential/sensitive information is sent to the mailbox of the person or persons who are authorised to see that information, and that no unauthorised persons have access to that mailbox/those mailboxes.

Before sending or receiving confidential/sensitive emails, confirm the email address with the other party, spelling any words that may cause errors. Use must be made of the e-mail "Tracking Options" where available, to notify that a message has been delivered and/or read. Otherwise the sender must be telephoned to confirm receipt. A copy of the e-mail and its attached documents must be stored appropriately within manual and/or electronic records, and the original email deleted from both the inbox and deleted items.

All members of staff should be mindful of using the 'reply all' and 'cc' buttons to prevent against other people receiving information unnecessarily. There must be a justified reason for anyone to be copied into or sent PID.

Third Parties

The risks associated with engaging a third party will be identified, assessed and managed and due diligence shall be undertaken in any such proposals. Where third parties are used to manage information or information processing facilities, a formal contract shall be in place that defines the information security requirements of the relationship.

The delivery of the contracted services is monitored, and formal procedures are in place to manage change and the identification, reporting and management of information security incidents. Contracts with third parties shall provide Oxona Healthcare with the right to audit the third party. All contracts with third parties that will process data on behalf of Oxona Healthcare will contain the relevant contractual clauses outlined within the GDPR.

Privacy by Design and Privacy Impact Assessments (DPIA)

Oxona Healthcare will act in accordance with the GDPR by adopting a privacy by design approach, which will seek to ensure that Oxona Healthcare have considered and integrated data protection into processing activities where required.

The GDPR does not require a DPIA to be carried out for every processing operation that may result in risks to the rights and freedoms of natural persons. The carrying out of a

OXONA HEALTHCARE

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

DPIA is only mandatory where a processing is "likely to result in a high risk to the rights and freedoms of natural persons". It is particularly relevant when a new data processing technology is being introduced.

DPIAs will be used to identify the most effective method of complying with Oxona Healthcare data protection obligations when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. High risk processing includes, but is not limited to, the following:

- a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences
- systematic monitoring of a publicly accessible area on a large scale.

In risk management terms, a DPIA aims to manage risks to the rights and freedoms of natural persons, using the following three processes, by:

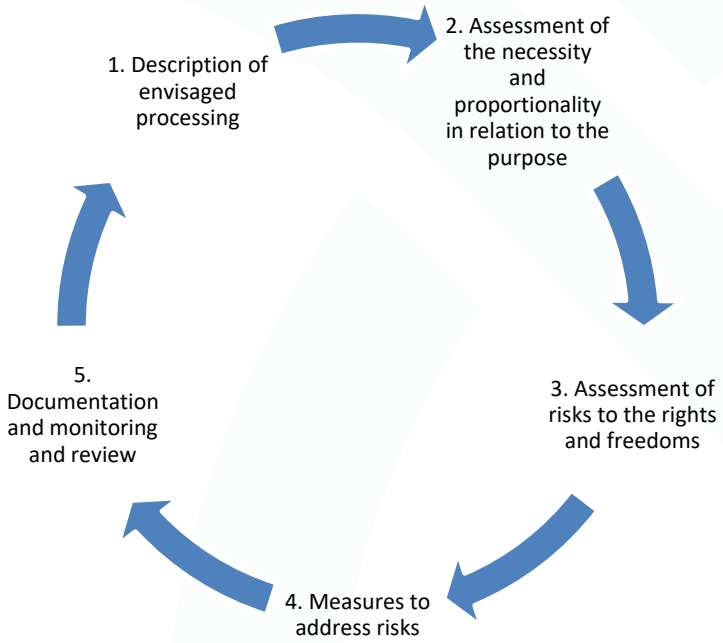
- establishing the context: taking into account the nature, scope, context and purposes of the processing and the sources of the risk
- assessing the risks: assess the particular likelihood and severity of the high risk
- treating the risks: mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

Oxona Healthcare will seek to ensure that all DPIAs include the following information:

- a description of the processing operations and the purposes
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an outline of the risks to individuals
- the measures implemented in order to address risk.

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk



Patient Confidentiality

For further information specifically relating to patient confidentiality, please refer to the Patient Confidentiality Policy.

Standards for Completion of Medical Records

Oxona Healthcare only uses GDPR compliant electronic medical records which are clear in content and completed as soon as is possible after the consultation or event, providing current information on the care and condition of the patient.

All entries in medical records are date stamped and signed electronically. Amendments cannot be made after 24 hours.

. Medical records should identify problems that have arisen, and subsequent actions taken to rectify them. They should also record other persons present during any visit/appointment/consultation. In the event of this being a student or any other members of staff observing the visit/appointment/consultation, there should also be a record of the service user's consent.

Medical records should be factual, consistent, clear and accurate and written in a way that the meaning is clear. They should not include jargon, meaningful phrases, irrelevant speculation and offensive subjective statements. They should be formulated, wherever possible, with the involvement of the patient and/or their relatives in terms that they can understand.

Abbreviations in care records should only be used where this is first explained in the notes to identify what the abbreviation is.

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Roles and Responsibilities

The Data Protection Officer has overall responsibility for information governance within Oxona Healthcare. The Data Protection Officer is responsible for:

- informing and advising Oxona Healthcare and individuals associated with the business about their obligations to comply with the GDPR and relevant data protection legislation
- monitoring compliance with the GDPR and other data protection legislation, including managing internal data protection activities and ensuring that relevant training is available for all members of staff
- acting as the first point of contact for regulatory authorities and for data subjects
- investigating any breaches of the GDPR, reporting such breaches as appropriate and ensuring that appropriate arrangements are put in place to prevent similar breaches occurring in the future.

The Registered Manager is responsible for:

- carrying out and keeping up to date a personal data audit
- ensuring that this policy is implemented within their team and that all members of staff receive Information Governance Training in line with this Policy.

Monitoring and Compliance of the Policy

The Data Protection Officer is responsible for ensuring the ongoing relevance of this Policy and for monitoring the consistency of its application. This will primarily be done via face-to-face supervision sessions.

This policy will be routinely reviewed every 3 years by the Data Protection Officer, or earlier if there are any changes in legislation.

Legislation and Guidance

General Data Protection Regulation 2016

Data Protection Act 2018

Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003

Information Commissioner's Office Guide to the General Data Protection Regulation: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

The Information Governance Review: Information to Share or not to Share: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

St Luke's Hospital
Headington,
Oxford,
OX3 7PF

01865 965 027
oxonahealth.co.uk
reception@oxonahealth.co.uk

Compliance

Safe	**S6:** Are lessons learned and improvements made when things go wrong
Well-led	**W2:** Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed. **W3:** How are the people who use the service, the public and staff engaged and involved