OR06 Information Governance and Data Protection Policy

Document Version Tracking					
Version	**Date**	**Revision Description**	**Author/Editor**	**Assured by**	**Review cycle**
1	July 2010	Updated due to company reorganization and legislation change	Head of Finance		
2	Jan 2012	Review	Service Manager		
3	Dec 2013	Updated section 8	Service Manager		
4	Oct 2014	Review	HR Manager		
5	Mar 2015	Updated due to changes in external requirements and compliance with IG Toolkit	Manager Quality & Performance		
6	Mar 2019	Updated due to General Data Protection Regulations (EU) and new Data Protection Act 2018	Jess Daer, Quality & Compliance manager & Liz Thompson, Head of Quality & Compliance	Board	2 years
Note: This document is electronically controlled and is published as a PDF and should not be altered. The master copy is maintained by the Policy Lead within the document library and should be used only for an authorised review.					

Table of Contents: Information Governance and Data Protection Policy

Table of Contents: Appendices

Index of associated SOPs

SOPO02 – Information Governance Handbook v1

SOPO03 – Subject Access Process Guidelines v3

SOPO04 – Data Protection Audit v1

Introduction

The Data Protection Act (DPA; 2018) and the General Data Protection Regulation (GDPR) sets the legal framework, by which we can process personal information. It applies to information that might identify any living person. The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential. The Human Rights Act (1998) article 8 provides a person with the right to respect for private and family life. The key rights provided by this legal Framework are also set out in the NHS Constitution (section 3A).

This policy provides a guide to the key elements of the legal framework governing information handling, outlines the responsibilities for managers and staff in relation to data protection, information governance and data quality and, in conjunction with the Information Governance Handbook, provides guidance on all aspects of information handling.

Data Protection Principles

The Data Protection Act (2018) defines six Data Protection Principles; which all processors of personal information must abide by. The 6 principles are:

1. Processing shall be lawful, fair and transparent
2. The purpose of processing shall be specified, explicit and legitimate
3. Personal data processed shall be adequate, relevant and not excessive
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary
6. Personal data shall be processed in a secure manner

GDPR also introduced the principle of **accountability**; EDP must demonstrate compliance, ensuring GDPR strategy is auditable and evidenced and all our decision-making is recorded.

EDP ensures that appropriate policies, procedures, management accountability and structures are in place and provide a robust governance framework for information management.

1. Statement

1.1 EDP holds and processes personal information about its service users, employees, and other individuals for various purposes (e.g. the provision of services or for administrative purposes, such as HR and payroll).

1.2 EDP is committed to treating people who use our services, staff and other stakeholders with the utmost respect. EDP recognises that unauthorised disclosure may put an individual at risk of harm. We are committed to meeting our legal obligations and associated requirements concerning data protection and information governance. EDP will ensure there is a nominated person with overall responsibility for data protection.

1.3 EDP will ensure:

i People are effectively informed and know how to access their information and exercise their rights.
ii Clinical and corporate information is managed in accordance with mandated and statutory requirements.

1.4 We will make staff aware of the consequences of failing to adequately protect information. Any organisation that processes personal information faces severe consequences, including fines of up to 10 million Euros for breaching the Data Protection Act, and/or significant reputational damage. Individuals can also be held personally and criminally accountable.

1.5 EDP ensures the appropriate technical and organisational measures are in place to protect against unauthorised access to data.

2. Scope

2.1 This policy is a core policy and thus applies to all staff. In the context of this policy the term 'staff' is defined as all salaried staff, volunteers, students on placements, trustees and any other individuals accountable to EDP.

2.2 This policy also applies to staff employed by other organisations working in an EDP-led service or working with EDP data.

3. Aims and Objectives

3.1 The objectives of this policy are:

- To demonstrate the ways in which we ensure that patient and staff data is handled effectively and securely
- To promote best practice and innovative use of personal information, especially to inform care and research
- To ensure that we understand our responsibilities and obligations.

4. Definitions

Term	Definition
Personal data and/or information	Any information relating to an identifiable living person who can be directly or indirectly identified in particular by reference to an identifier.
Special category personal information (or data)	Personal data consisting of information as to: the racial or ethnic origin of the data subject, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), physical or mental health or condition, sexual life, the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
Data controller	The person (or company) who determines the purposes for which and the manner in which any personal data are, or are to be, recorded.
Data flow	A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.
Data processor	Any person who processes data on behalf of the data controller.
Direct care	The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider. Examples include assessment, performing procedures and implementation of a care plan.
Confidential information	Any information that relates to services users, staff, their family and friends, however stored.
Duty of confidence	A duty of confidence, a common law principle, arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.
Explicit consent	A form of consent normally given orally or in writing and is where a service user makes a clear and positive indication that they understand the consequences of what they are agreeing to and are content with these consequences. For data protection purposes, this must clearly set out how the information is going to be used and how the person can withdraw that consent.
Information governance	A combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards.
Legitimate relationship	A relationship that exists between a service user and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.
Processing	This term covers the collection, recording or holding of information or data, or carrying out any operation or set of operations on the information or data, including but not restricted to alteration, retrieval, disclosure and destruction or disposal of the data.

Non care or secondary purpose	Purposes other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

5. Responsibilities

5.1 The Board is ultimately responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

5.2 The Chief Executive Officer has overall responsibility for Information Governance, Information Security and this Policy within EDP. Implementation of and compliance with this Policy is delegated to the Senior Information Risk Officer (SIRO), Caldicott Guardian and to the members of the Performance, Quality and Compliance Committee and team.

5.3 The Head of Compliance is the appointed Data Protection Officer (DPO) and has ultimate responsibility for ensuring compliance with the Data Protection Act (2018), the General Data Protection Regulation, Human Rights Act (1998) and the Common Law Duty of Confidentiality. The Head of Compliance is responsible for day to day Information Governance issues; developing and maintaining Information Governance policies, standards, procedures and guidance, coordinating Information Governance in the Agency, and raising awareness of Information Governance.

5.4 The Director of Services is the Caldicott Guardian for EDP. (The 'conscience' of the organisation, providing a focal point for service user confidentiality, information sharing issues and advising on the options for lawful and ethical processing of information as required). The Director of Services is the designated Senior Information Risk Owner (SIRO), who takes ownership of EDP's information risk policy. The SIRO acts as an advocate for information risk on the Board. The SIRO also reports annually to the Board on IG performance.

5.4 The Quality and Compliance Manager is accountable to the Head of Compliance and supports both the DPO and the Caldicott Guardian to ensure appropriate use of personal information. The Quality and Compliance Manager is responsible for assisting the Head of Compliance and the SIRO with reporting and analysing IG incidents, e.g. data protection/confidentiality breaches, reporting and investigation; and for assisting staff on queries relating to information sharing and confidentiality.

5.5 The Directorate are designated Information Asset Owners (IAOs) with responsibility for providing assurance to the SIRO that information, particularly personal information, is effectively managed within their Directorate/Department. Directors are responsible for data quality within their respective directorate areas.

5.6 Service Managers are responsible for all staff working within their service being aware of their personal responsibilities. They must ensure IG policies and procedures are followed, ensure staff are trained to recognise actual or potential security incidents and take steps to mitigate those risks, consult their DPO on incident management, and ensure that data processing registers are accurate and up to date. Service Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

5.8 Team Leaders will monitor staff practice and discuss any issues relating to confidentiality with regard to service delivery at supervision and team/clinical/ multi-disciplinary meetings. They will discuss with Service Managers and appropriate leads decisions in situations where it is not clear as to whether or not information should be shared without the consent of the person to whom the information relates to This will be documented for auditable and operational purposes (e.g. in service user notes/supervision records).

Individual responsibilities

5.9 All staff (including agency staff, honorary contracts, management consultants etc.) who use and have access to EDP personal information must understand their responsibilities for data protection and confidentiality, which include adherence to policy and confidentiality clauses in the contract, the Data Protection Act, Common Law of Confidentiality, and professional obligations e.g. Confidentiality NHS Code of Practice and professional codes of practice. All staff must process data in line with the law and as directed by EDP policy.

All staff are responsible for ensuring information that they generate/review is legible, complete, accurate, relevant, accessible and recorded in a timely manner. All staff are responsible for asking questions and raising concerns to their line manager if they feel unsure.

6. Information Governance

There are 4 key interlinked strands of information governance:

- Openness
- Legal compliance
- Quality assurance
- Information security

6.1 Openness

- Non-confidential information about EDP and its services should be available to the public through a variety of media in line with the charity's commitment to accountability and transparency.
- EDP will establish and maintain policies to ensure compliance with the Freedom of Information Act.
- EDP will undertake or commission annual assessments and audits of its policies and arrangements for openness.
- Service users should have ready access to information relating to their own care, their options for treatment and their rights as service users.
- EDP will have clear procedures and arrangements for liaison with the press and broadcasting media.
- EDP will have clear procedures and arrangements for handling queries from patients and the public.

6.2 Legal Compliance

- EDP regards all identifiable personal information relating to service users as confidential.
- EDP will undertake or commission annual assessments and audits of its compliance with legal requirements.
- EDP regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- EDP will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality.
- EDP will establish and maintain policies for the controlled and appropriate sharing of service user information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act, Mental Capacity Act

6.3 Information Quality Assurance

- EDP will establish and maintain policies and procedures for information quality assurance and the effective management of records.

- EDP will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Wherever possible, information quality should be assured at the point of collection.
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- EDP will promote information quality and effective records management through policies, the Information Governance Handbook and training.

6.4 Information Security

- EDP will ensure effective and secure management of its information assets and resources.
- EDP will undertake or commission annual assessments and audits of its information and IT security arrangements.
- EDP will promote effective confidentiality and security practice to its staff through policies, procedures and training.
- EDP will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

Regarding information security, EDP will ensure the following:

6.4.1 Security - Assets will have named custodians who will be responsible for the information security.

6.4.2 Access – Only authorised persons with a business need will be given access to systems. Access will be managed according to approved and documented processes.

6.4.3 Equipment - All assets will be protected with the appropriate threats and environmental hazards, including software. All staff are responsible for protecting equipment against malicious intent and staff will not install any unauthorised software or disable protective features.

6.4.4 Risk assessment – identified risks will be held on the risk register and managed formally.

6.4.5 New systems – a security plan and risk assessment will be conducted prior to the implementation of any new system. Changes to existing systems are subject to the same process.

6.5.6 Intellectual property – all products will be properly licensed.

6.5.7 Business Continuity – business continuity plans will consider risks and impact of restricted access to information and plan accordingly.

7. Data Quality

7.1 EDP is committed to ensuring the quality of its data, in order to deliver the best possible service. Risks of inaccurate data include potentially serious consequences for individuals or the organisation.

7.2 Data Quality is essential for:

- Efficient delivery of service e.g. by ensuring that people are given appointments based on clinical priority and length of waiting time
- Clinical governance and minimising clinical risk e.g. ensuring the right service is offered to the right person
- Management information to enable decisions to be made based on sound information, operational and strategic factors and local and national factors.
- Performance measurement against national trends and trends over time, so that we can continually improve
- As a foundation on which future investment and strategic decisions will be based.
- To support clinical audit and research and development, with a view to improving service delivery
- All staff need to be able to rely on the accuracy of the information available to them, to provide timely and effective services regardless of whether they are service user facing or central support functions.

7.3 To achieve this, all staff need to understand their responsibilities regarding accurate recording of data.

<u>Data Quality Standards</u>

- **Accurate and up to date:** All data must be correct and accurately reflect what happened.
- **Valid:** Data should be within an agreed format which conforms to recognised national or local standards. Wherever possible, computer systems should be programmed to only accept valid entries.
- **Complete:** Data should be captured in full. All mandatory data items within a data set should be completed
- **Timely:** Data should be collected at the earliest opportunity.
- **Defined and consistent:** The data being collected should be understood by the staff collecting it and data items should be internally consistent. Use of acronyms should be avoided where possible for clarity. Data definitions should be reflected in procedure documents.
- **Coverage:** Staff should be cognisant that if something is not recorded there is no auditable proof that something occurred, and as such could be challenged.
- **Free from duplication and fragmentation:** Data should be recorded once, and staff should know exactly where to access the data. Where a duplicate record is created, for example if a record is misplaced, records

should be merged once the original is found. Version control should be used for clarity where there could be multiple copies of a document.

- **Security and confidentiality:** Data must be stored securely and processed in line with relevant legislation and local policy in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share information ensuring they comply with national and local requirements, policies and procedures.

7.4 Data subjects have the right to see a copy of information about them and, if they believe the information in inaccurate, they can request an amendment. See the Subject Access Request Process for more information.

8. Implementation

8.1 Informing People using services

8.1.1 At the earliest opportunity, and before the interventions commence, the worker will explain responsibilities regarding confidentiality to the individual using EDP's services. They will explain how information will be kept confidential and when and what they would need to share, including the role of consent and the other lawful bases for sharing information. This should be done in clear language that can be easily understood. If at any point it seems appropriate to repeat this to the individual to help them and reaffirm working practice then it should be repeated. Refer also to P22 Service User Rights and Responsibilities Policy.

8.1.2 All individuals must be advised that information is confidential to the service, and not to the individual worker, and the operational reasons for this.

8.1.3 All written agreements regarding consent will be signed and dated by service users and staff and kept in the care record.

8.1.4 All service users will be provided with a 'How we use your data' information leaflet that explains in detail how their data is processed, their rights and processes to exert those rights. Additional information regarding a service user's right to confidentiality and access to their records should be readily available to service users if requested and affixed in public areas within the service

8.1.5 If workers are in doubt over any instance, they should always consult with their line manager.

8.1.6 In Media work, EDP will not use any information that could identify a service user unless they have their express permission and the service

user has signed a disclaimer form. Where a service user does agree to be named in any of this work, the risks to them doing so should be clearly outlined and the worker needs to be satisfied that these have been understood. In training or education this will also be done wherever practical.

8.1.7 Where a request to share information cannot be fulfilled, staff should be able to clearly and respectfully explain the reasons why they cannot share information. Issues should be escalated to the line manager.

8.2 Sharing information

8.2.1 There are six lawful bases under which EDP may process and share information. Refer to the Information Governance Handbook for more information. These are:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

8.2.2 Where a service user gives consent for us to share their information we are processing their data under the lawful basis 'consent'. Occasionally EDP may need to share information where there is no consent. Providing there is an alternative lawful basis, staff may share information. Refer to the Information Governance Handbook for practical examples, including safeguarding, where staff may need to use an alternative lawful basis.

8.2.3 All information sharing decisions must be documented in the care record.

8.2.4 Where information has been shared without consent, under an alternative lawful basis, data subjects should be informed and the decision making process explained, unless to do so would put either the data subject or a third party at risk of harm.

8.2.5 Consent must be documented in the care record using a signed How We Use Your Data form, which specifically states named organisations. Where it has not been possible to obtain written consent (for example the first interaction with the service user is by telephone), verbal consent is sufficient until there is an opportunity for written consent to be taken. Verbal consent must be documented in the care record.

8.2.6 Conversations about information sharing should be revisited regularly whilst a service user is engaged in treatment.

8.2.7 Where EDP routinely and justifiably shares personal data with other organisations, e.g. to support continuity of care, a data sharing agreement is to be drawn up between the affected organisations.

8.3 Access to Records

8.3.1 Staff should not access any files or documents for which they do not have appropriate authority to access.

8.3.2 Access to systems must be set up in such a way that ensures individuals only have access to information relevant to their role.

8.3.3 Staff do not have a right to access personal information about their relatives or friends held in records unless there is a legitimate reason for doing so and this has been approved by a line manager.

8.3.4 Any persons wishing to access records held about themselves (as a member of staff or service user) must submit a Subject Access Request.

8.3.5 See Appendix 2 Subject Access Request Process.

8.4 Keeping Personal Information Secure and Confidential

Staff are required to familiarise themselves with the Information Governance Handbook. The Handbook provides all staff (including contractors) with guidance on:

- ensuring the security of electronic and paper records,
- use of external storage devices;
- secure email and other methods of transferring information
- preventing unauthorised access to information
- password security
- clear desk policy
- access to systems
- deletion of data
- avoiding human error

8.5 Contractors

All people working with EDP, whether as paid employees, in a voluntary capacity, or as contractors are required to sign a Confidentiality Contract to the Service (see Appendix 3).

8.6 Use of Service user data for Non-Healthcare Purposes

8.6.1 Use of service user personal data for non-healthcare purposes typically falls into the categories of Clinical audit, Research or Service evaluation. This use of service user information must also comply with the DPA and Caldicott principles.

8.6.2 Clinical audit (usually conducted by those involved in service user care, and overseen and approved by the Performance, Quality and Compliance Committee) - Where an audit is to be undertaken by a member of EDP staff, service user identifiable information may be used. However, if this is to be shared outside of EDP, consideration must be given to seeking consent or how this processing falls under other lawful basis.
Audits may be conducted by bodies which regulate our services such as the Care Quality Commission (CQC).

8.6.3 Research - The use of service user identifiable information for research, by an external body or in partnership with an external body, requires explicit informed consent. When seeking consent for disclosure, you must ensure that the service users are given enough information to allow them to make a considered and informed decision. Specifically, they should be informed of the reasons for the disclosure, the way that it will be made and the possible consequences. The exact amount of disclosure and the identity of those who will receive it should also be explained.

External research bodies must not be given direct access to the data without following a process that scrutinises the appropriateness of this.

8.6.4 If a service user cannot be contacted to give consent, it should not be assumed that their care details can be used for research purposes.

8.6.5 Where explicit consent is not present, anonymised data which cannot identify individuals may be used for research purposes.

8.6.6 Test profiles must be used for systems testing where possible. If the use of live data is unavoidable, the persons conducting the testing with access to the live data must be employed by EDP or have signed the relevant contractor agreement.

8.7 Requests for disclosure of information to third parties

Please see SOPO03 Subject Access Request Guidelines for further information. Please contact the Compliance Team (Head of Quality and Compliance and Quality and Compliance Manager) or Caldicott Guardian with any queries.

8.8 Disposal of Confidential Information

The effective management and disposal of waste materials that contain confidential person identifiable information, or confidential corporate information, is the responsibility of all staff.

EDP will ensure that appropriate resources are available for the disposal of confidential waste and will monitor the implementation of this.

8.9 Data Protection Impact Assessments (DPIA)

8.9.1 Any new (or significantly changed) system, process or policy which involves the processing of personal data must be subject to a DPIA at an early stage in the project. The aim is to identify any risks to an individual's privacy and ensure the risks are minimised to an acceptable level. The DPIA (identifying what data is processed, who has access to the data, where data is stored) should be approved by the Compliance Team. Any risks which are deemed high and cannot be mitigated against would result in the processing being stopped and/or might be referred to the ICO by the Compliance Team. Refer to Appendix 2 Privacy Impact Assessment Template.

8.9.2 External suppliers involved in processing and/or storing the data (e.g. EDP IT provider, new data storage providers) will be expected to demonstrate adherence to national standards of information security, e.g. 'satisfactory' Data Security and Protection (DSP) Toolkit submission, ISO 27000 certification.

8.10 Breach of Policy

Breaches should be reported immediately to the line manager, DPO and Compliance Team. Where an incident has occurred, this should be also reported via the MyEDP incident reporting system as an information governance incident.

8.11 Disciplinary Proceedings

8.11.1 In an instance where an individual worker has been found to have inappropriately shared personal data, this should be reported as an incident and the Team Leader/Manager must address this. The action taken should take into account the effects on the Service, the organisation and the individual concerned. The Data Protection Officer must also be notified of all Data Breaches.

8.11.2 EDP operates a no-blame culture in respect of genuine human error and focusses on improving systems to reduce risks of breaches. However, deliberate acts including sharing or accessing personal data without justifiable reason or failing to safeguard confidential information may constitute gross misconduct and may result in dismissal for a first offence.

8.11.3 Staff should note that all systems can be monitored and audited, so any unauthorised access will be recorded and can be evidenced.

8.11.4 Any reported confidentiality breach will be raised with the relevant Director and may be taken forward in line with EDP's Disciplinary Policy.

8.12 Legal Proceedings

The Information Commissioners Office has a number of tools available for taking action to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The ICO also has the power to serve a monetary penalty notice on a data processor and controller. Individuals can be held criminally responsible for gross breaches.

8.13 Training and Policy Awareness

- The induction process will cover data protection and information security expectations.
- Expectations will be made clear through contracts of employment and job descriptions.
- IG training (e-learning) is mandated at corporate induction and thereafter annually with a minimum target of 95% completion across EDP. Staff are required to complete the mandatory e-learning before being given access to systems.
- Training needs will be reviewed annually through the workforce development planning process which will consider the needs of all staff and of specific roles such as the Caldicott Guardian, SIRO, DPO and Service Managers. Details of training to support delivery of this document are covered in EDP's Training Needs Analysis.
- Where additional training needs identified for individuals or groups (e.g. through monitoring and audit activities) these will be addressed appropriately.
- A copy of this policy and relating policies and procedures will be posted on EDP's Intranet (MyEDP) and no hard copies should be retained.
- All staff are made aware of their responsibilities for Information Governance at induction and annually as part of their mandatory training and development as well as through the IG Handbook which is regularly updated.

- The Compliance Team ensure regular promotion of data protection and confidentiality matters through EDP e-news, briefings, training, posters, leaflets and committees.
- Staff will receive relevant dedicated training in the use of specific service data collection systems

9. Monitoring and Reviewing

9.1 Monitoring compliance with Data Protection and Information Governance obligations is essential for EDP to protect the rights of service users, staff in compliance with the law and contractual obligations. It is also plays an important role in service improvement. It will be monitored through audit, supervision, staff and service user surveys, incident reports, complaints, feedback and spot checks - the outcome of which will be reported through EDP's defined committee structure and management processes.

9.2 This policy will be reviewed every 3 years or following any change in relevant legislation, whichever is sooner.

Appendix 1 - External Contractor Confidentiality Agreement

This form is intended for use by contractors or third parties not directly employed by EDP who are working on our premises or may otherwise come into contact with our service users or sensitive information.

EDP is committed to addressing substance misuse, improving the health, social well-being and quality of life of individuals, their families and communities affected by their own and others' substance misuse. EDP maintains the highest standards around data protection and confidentiality.

It is recognised that while undertaking your duties you may be privy to sensitive information. You may, for example, become aware of the names of service users attending EDP or you may recognise someone you know. It is imperative that you do not divulge any information regarding our service users under any circumstances to unauthorised persons.

The Data Protection Act 2018 regulates the use of all personal information and includes electronic and paper records of identifiable individuals (patients and staff). If you are found to have used any information you have seen or heard whilst working within EDP inappropriately, you (and your employer or the organisation you represent, if relevant) may face legal action.

Any questions regarding data protection should be directed to a member of EDP staff or the manager of the service in which you are working.

I agree to:

- Undertake the work/duties as agreed in line with EDP's Data Protection requirements
- Never disclose confidential information to unauthorised persons
- Never to copy confidential information for an unauthorised reason
- Never to remove confidential information from the premises

Name	
Position	
Organisation	
Date	

EDP Privacy Impact Assessment

Appendix 2 - Privacy Impact Assessment

Conducting a PIA is a requirement set out by Department of Health (DH) and Connecting for Health in the Information Governance Toolkit. The purpose of conducting a PIA is to:

- Meet and exceed legal requirements.
- Identify and manage risks to address any privacy issues.
- Avoid loss of trust and reputation by minimising privacy deficiencies.
- Inform the organisation's communications strategy by consulting with stakeholders.
- Avoid unnecessary costs by performing a PIA at an early stage in project.
- Avoid 'bolt on' solutions which could be more expensive in the longer term.

Not every project or system will require a PIA. The ICO sees PIAs being used only where a project has a wide scope, or will use personal information of such a nature, that there would be genuine risks to the privacy of the individual, new and intrusive technology is being used, or where private or sensitive information which was originally collected for a limited purpose is going to be reused in a new and unexpected way.

Project Title:		Service / Dept:	
Assessment Author:		IG Lead:	
Date:		Chief Executive:	
Reviewed by:		Date:	

Part Privacy Impact Assessment (Questions 1-10)

IDENTIFYING AND ASSESSING THE RISKS	RISK LEVEL	CONTROLS FOR MANAGING THE RISKS	REMAINING RISK
1. Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?			
2. Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management?			
3. Might the project have the effect of denying anonymity or converting transaction, identity authentication or identity management process?			
4. Does the project involve multiple organisations, whether they are private, voluntary or statutory sector organisations, e.g., outsource service providers or business partners?			
5. Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?			

6. Does the project involve new or changed handling of a considerable amount of personal data about each individual in the database?			
7. Does the project involve new or significantly changed handling of personal data about a large number of individuals?			
8. Does the project involved new to significantly changed consolidation, intern-linking, cross-referencing or matching of personal data from multiple sources?			
9. Does the project relate to data processing which is exempt from legislative privacy protection?			
10. Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?			

NOTE: If the risk level has been identified as HIGH to any of the above questions you will need to carry out a FULL Privacy Impact Assessment in consultation with the Calidcott Guardian.

OR06 – Information Governance and Data Protection Policy **Version 6**		
Summary:	To understand our responsibilities and obligations to service users, staff and any other individuals who disclose personal information to the organisation under the Data Protection Act 2018 (DPA), the Common Law Duty of Confidentiality, best practice NHS Code of Practice: Confidentiality and Caldicott principles and the DSP Toolkit	
Related Legislation:	Data Protection Act 2018 (DPA) General Data Protection Regulation 2018 Common Law Duty of Confidentiality NHS Code of Practice: Confidentiality Caldicott principles DSP Toolkit Children Act 1989, 2004 Police and Criminal Evidence Act 1984 Counter-terrorism and Security Act 2015 Mental Health Care Act 2017	
Related Policies:	HS01 Health and Safety at Work Policy HR07 Whistleblowing (Confidential Reporting) Policy OR10 information Security Policy P07 Record Keeping Policy P11 Working with Young People Policy P15 Safeguarding Children Policy P16 Safeguarding Vulnerable Adults Policy and Procedure P22 Service User Rights and Responsibilities Policy	
Next Review Date:	18-06-2021	
Approved by (Head of Department):	Julie Howes, Director of Services and Helena Freeman, Director of Finance	**Date:** 21/05/2019
Ratified by:	Board	**Date of meeting:** 04/06/2019
Date issued:	18-06-2019	
Author:	Jess Daer, Quality & Compliance Manager & Liz Thompson, Head of Quality & Compliance	
Reviewers/contributors:	n/a	**Date:**