Willingham-by-Stow

Information Governance
Subject Access Policy

Documentation Control:

Version	Version 02
Ratified by	The Partners
Date Ratified	19/04/2022
Author(s)	PCU
Responsible Committee/Officers	SIRO
Date Issue	19/04/2022
Review Date	30/06/2023
Intended Audience	All Practice Staff

Further Information about this document:

Name	WBS Subject Access Request Policy GP V02.docx
Contacts(s) for further information about this document	Ian Hammerton
This document should be read in conjunction with	Information Governance Framework
Published by	Willingham-by-Stow
Copies of this document are available from	Ian Hammerton

Version Control:

Version Number	Reason	By	Date
01	For DSP V03 submission	Peter Case-Upton	29/03/2021
02	Updates required for Version 04 of the DSP Toolkit	Peter Case-Upton	19/04/2022

Contents

1. Introduction

Willingham-by-Stow, (the Practice), recognises the individual's right of access to their recorded information (a Subject Access Request (SAR)) and in some cases, to information relating to other people. The Practice will ensure that adequate provision is given to service users and staff to exercise this right.

This Policy describes how the Practice will achieve compliance with the key legislation that provides access to personal information.

The Data Protection Act 2018 (and the General Data Protection Regulation), regulates the processing, including disclosure of information relating to living individuals. The Act gives the individual (data subjects) or their authorised representatives the right to apply to view or have copies of personal data held about them, including health and social records, (subject access rights) and personnel records.

The basis of this framework includes the following requirements of the new UK GDPR regulations: -

- An all-inclusive information asset register with data flow mappings must be maintained and processes developed to ensure the assets are current
- The legal basis for the processing of information are required
- Consent with suitable 'opt in' and 'opt out' conditions must be included
- The Information Commissioners' Office (ICO) must be notified of data breaches within 72 hours
- Increased fines for failure to comply with the regulations will be imposed
- Fair processing notices will require updating to inform users of UK GDPR implications
- The introduction of a Data Protection Officer (DPO) role to the Practice will be mandated
- There will be changes to individual's rights over the way data is stored
- Timescales for Subject Access Request responses etc. will be decreased
- Evidence of UK GDPR compliance must be made transparent and available

UK GDPR applies to 'data controllers' and 'data processors'. The definitions are a part of the Data Protection Act 2018 – the controller says how and why personal data is processed and the processor acts on behalf of the controller.

The Practice as a Data controller will not be relieved of its obligations where a processor is involved and the UK GDPR will place further obligations on the Practice to ensure all contracts with data processors comply with UK GDPR.

The Practice recognises that where there is legitimate interest, information relating to the deceased is accessible through the access to Health Records Act 1990. (if applicable)

This Policy should be read in conjunction with the related policies listed in section 24.

2. Aim

The purpose of this policy is to establish the Practice's responsibilities as the designated data controller under the Data Protection Act 2018 and the UK version of UK GDPR, to comply with and process Subject Access Requests.

This document provides policy statements to the staff processing such requests and the data subjects themselves and:

- describes how the Practice will comply with the law
- provides assurance on lawful practice
- establishes the roles and responsibilities of staff in the processing of requests
- establishes that processes will be in place to support this policy

3. Definitions

The key definitions applicable to this policy are as follows:

Health/Medical Record	The Data Protection Act 2018 defines a health record 'as a record consisting of information relating to the physical or mental health or condition of an identified individual made by or on behalf of a health professional in connection with the care of that individual'. The record may be held in computerised or manual form or in a combination of both. Item 35 of UK GDPR states that personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.
The Data Subject	An individual who is the subject of the information (service user/member of staff)
The Data Controller	A person (or organisation) who determines the purposes for which and the manner in which personal data, is processed
The Data Processor	in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Subject Access Rights	Individuals can make an application in writing to gain access to information held or processed about them
3rd Party	A person identified in the health/medical record other than the data subject or a health professional
Service users Personal Representative	Defined as the executor or administrator of the deceased estate.

Caldicott Guardian	Designated by the Caldicott Committee as responsible for overseeing the arrangements for the use and sharing of clinical information.
Data Protection Officer	The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their data (b) to monitor compliance with this Regulation, data protection provisions and with the policies of the controller or processor including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
Senior Information Risk Owner	The role of the Senior Information Risk Owner (SIRO) was created to provide board-level accountability and greater assurance that information risks are addressed. The SIRO ensures that information risks are treated as a priority for business outcomes. The SIRO also plays a vital role in getting their organisation to recognise the value of its information enabling them to use it effectively.
Statutory Gateway	Permits disclosure of information
Access to Health Records Act 1990	This Act has been repealed to the extent that it affected the Health/medical records of living service users and is now only in force in respect of deceased service users. Applies to records created since 1st November 1991
Data Protection Act 2018	An Act that regulates the processing of information relating to living individuals including the holding use or disclosure of such information
General Data Protection Regulation	The primary objectives of the UK GDPR are to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.
Freedom of Information Act 2000	An Act to make provision for the disclosure of information held by Public Authorities (not applicable to private organisations)
Access to Medical Reports Act 1988	An Act to make provision for the individual to access medical reports written by a health professional for the provision of a service

4. Responsibilities

4.1 The Board

The Board has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

The Organisation has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements

4.2 Caldicott Guardian

The Organisation Caldicott Guardian is Dr Daniel Lane and is responsible for the confidentiality of person identifiable information as designated in the Caldicott Report and for the information governance agenda, which incorporates data protection.

4.3 The SIRO and Information Governance (IG) Lead

Ian Hammerton is the Practice's IG Lead and the Senior Information Risk Owner (SIRO), and is responsible for overseeing the application of this Policy and its principle within the Practice. The IG Lead will ensure that there are robust processes in place to respond to subject access requests from staff and service users.

4.4 Data Protection Officer

A DPO is **mandatory** in the following three cases (UK GDPR Article 37(1)):

1. The controller or processor is a Public Authority or Body, or acting as one
2. The **core** activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a **large** scale
3. The **core** activities of the controller or the processor consist of processing on a large scale of **special categories** of data (i.e. highly sensitive, such as political affiliation or sexual preference) or personal data relating to criminal convictions and offences

According to Working Party 29, "**Core Activities**" can be considered as "the key operations necessary to achieve the controller's or processor's goals." i.e. The data processing is at the heart of the Practice's ability to operate, e.g. a hospital, or private security firm.
"**Large Scale**" is a fuzzy term and up to the data controller/processor to determine whether it applies to them, based on factors such as quantity of subjects, records, geography and duration of activity. Examples of large scale monitoring are hospitals, search engines, insurance company customer data. Examples that do not constitute large scale monitoring are the processing of data by an individual doctor or accountant, or the processing of personal data relating to criminal convictions and offences by an individual lawyer.

4.5 Records Management and Data Quality Lead

The Records Management Lead will be responsible for records management elements of compliance with this Policy on behalf of the Board and will receive reports on compliance with the subject access

provisions through the SIRO. The Data Quality Lead will be responsible for ensuring that data quality errors are maintained at an acceptable level. In addition, they will be responsible for the development of data quality reports.

4.6 Human Resources

The Human Resources department will provide information from staff records where that staff member has requested access to their personnel file, to comply with this policy. A member of the Human Resources department will review personnel files with the Corporate Services Manager before release to establish if any of the information may not be available for release.

4.7 Departmental Managers

Departmental Managers will ensure that their staff are aware of this Policy and comply with and support the operational procedures. Managers will make information readily available to The Records Management Lead to support the processing of subject access requests.

4.8 Staff

It is the responsibility of all permanent and temporary staff, students, volunteers and contracted staff to comply with data protection legislation, this Policy and the processes that support it. Several Practice Staff have been trained in SARS techniques

5. Subject Access Requests

The Practice will accept written requests, including e-mail, from a data subject in the provision of subject access. The Practice will make a standard access form available to the public/staff, where required, to assist the application - see Appendix B.

Telephone applications from an individual who is unable to make a written request may be accepted subject to strict conditions following the Department of Health Guidance for Access to Health Records 2010.

The Practice requires applicants to provide 2 forms of proof of identity one of which should be photo identification.

Where an application is made on behalf of a service user/member of staff the Practice will confirm that the consent of the individual had been obtained prior to any release.

Where an individual has not specified the information that they require the Practice will ask the applicant to refine the request.

Where an access request has previously been met and a subsequent identical or similar request is received the Practice will assess if a reasonable time interval has elapsed before providing the information.

5.1 Provision of Copies or Viewing Records

The Practice will ensure that a relevant professional is consulted prior to any release of information of a health-related nature. The Practice will require the professional to consider the following prior to the release of copies or the viewing of records:

- any serious harm to the physical or mental health or condition of the service user or, member of staff requesting access, or any other person
- the consent of any third party where the content relates to that third party who is not a health professional
- if it is reasonable to disclose without the consent of a third party

5.2 Medical Terminology and Viewing a Record

A health professional will be available during the viewing of a health-related record including occupational health records to respond to questions relating to any medical terminology.

A designated lay administrator will oversee the viewing of records where a health professional is not required.

5.3 Access to Records of the Deceased

Application to view or have copies of health-related records or occupational health records of the deceased will be considered under the Access to Health Records Act 1990.

The Practice recognises that it owes a duty of confidentiality to the deceased.

The Caldicott Guardian will be consulted on any proposed disclosure of information relating to the deceased and legal advice will be sought where necessary.

5.4 Access by Relatives of the Deceased

The Practice will consider access by a relative of the deceased to their health related or occupational health records. Where a request is made by a person who may have a claim arising out of the service user's death the Practice will require proof of such a claim before any disclosure is made.

The Practice will consider if a disclosure relating to the deceased's death would help a relative through the grieving process, subject to any refusal from the deceased prior to death.

Consideration will be given to requests from a living relative for information relating to a genetic or hereditary condition, subject to any refusal from the deceased prior to death.

5.5 The Personal Representative

The Personal Representative of the deceased has an unqualified right of access to the health-related record. The Practice will require proof of administrator/executor status before any disclosure is made.

5.6 Access to Children Records

The Practice considers that a person with parental responsibility is able to apply for access to a child's health related record where a health professional has made with due regard to the duty of confidence owed to the child, before any disclosure.

Young people aged 16 or 17 will be considered as adults in respect to their rights to confidentiality.

Due regard will be given to children under the age of 16 who have the capacity and understanding to make decisions about their own treatment and access to records.

5.7 Information Shared with Other Organisations

Where the Practice has legitimately shared identifiable information with other organisations and that organisation maintains its own records the Practice considers that subject access requests should be made directly to that organisation.

Where the Practice legitimately accesses another organisations system, subject access requests relating to information in that system will be referred to that organisation.

5.8 Application by Solicitors

The Practice will pay due regard to subject access requests made through a solicitor where the consent of the data subject has been provided. Consideration will be made to the information requested under the subject access provisions of the Data Protection Act 2018.

5.9 Statutory Disclosures

The Practice will consider application for access to health related and occupational health records and personnel records where there is a lawful requirement to comply.

5.10 Disclosures in Absence of a Statutory Requirement

Where there is no statutory requirement to comply with a request for access the Practice will consider applications on a case by case basis.

The Practice recognises that in all cases the public interest in disclosure must outweigh the duty of confidentiality owed to the deceased before any disclosure is approved.

6. Timeframe for Compliance

The ICO states that the time limit for issuing the information is one calendar month from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month. This means that if a SAR is received on 3rd September, the deadline for responding will be 3rd October (not 4th October as previously understood).

The Practice will inform applicants of any refusal to comply with requests as soon as possible within the given timeframe.

7. Request Log

Subject access requests including access to health related, personnel and occupational health records will be recorded in a log that will be used to demonstrate compliance with statutory timeframes and will provide assurance reports.

8. Amendments to Records

The Practice recognises that an opinion or judgment recorded by a health professional, whether accurate or not should not be deleted from a health-related record.

Where a data subject requests amendment to information in a health-related record or occupational health records the health professional concerned will be consulted.

Amendments will be made where both parties agree and the original information will be left clearly visible. An explanation and amendment date signed by the health professional will be added to the record.

Where a health professional considers disputed information to be accurate the Practice will ensure that a note recording the service user's disagreement will be added and that the date and signature of the health professional will be included.

Inaccuracies in personnel records will be considered with a Senior Manager in the HR department and will be amended if appropriate and signed and dated by the Senior Manager

9. Service Users/Former Members of Staff Living Abroad

Service users or former members of staff, who are now living outside of the UK, will be given the same rights of access under the Data Protection Act 2018, where the records of treatment occupational health or personnel records are still held by the Practice.

Original medical or occupational health or personnel records will not be transferred abroad. A copy or summary of record will be provided, subject to the fees stipulated in Appendix A.

10. Freedom of Information Act 2000 (if applicable)

The Practice will consider any requests for information which constitutes personal information to be exempt from disclosure under the Freedom of Information Act 2000 if:

- disclosure would contravene any of the Data Protection principles
- Where information has been provided in confidence.
- Where a duty of confidentially is owed to the deceased.

Private organisations do not need to respond directly to FOIs but may, on occasion, assist commissioners with such requests

11. Access to Medical Reports Act 1988

Applications to view Medial Reports following Insurance or employment medicals with be considered with regard to the Access to Medical Reports Act 1988. (if applicable)

12. Section 29 Access Requests

Section 29 of the Data Protection Act provides an exemption in Law to access person identifiable information without seeking the consent of that individual for the purpose of investigating serious crime, fraud and taxation purposes.

The Practice will consider Section 29 applications on a case by case basis.

Where the Practice deems it acceptable to disclose under a section 29 request it will release sufficient information for the purpose but not excessive to the purpose.

The Practice recognises that subsequent to the refusal of a Section 29 request the Police may seek a Court Order which requires the disclosure.

Under UK GDPR[1] the relevant Articles associated with subject access of records include:-

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject
Article 13: Information to be provided where personal data are collected from the data subject
Article 14: Information to be provided where personal data have not been obtained from the data subject
Article 15: Right of access by the data subject
Article 16: Right to rectification
Article 17: Right to erasure ('right to be forgotten')
Article 18: Right to restriction of processing
Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20: Right to data portability
Article 21: Right to object
Article 22: Automated individual decision-making, including profiling
Article 23: Restrictions

13. Complaints

Information will be available to service users and staff detailing how to apply for access to health related, occupational health, and personnel records and will detail the complaints process.

The Practice will initially try to resolve any complaints regarding subject access requests through informal discussion. If unresolved a formal complaints process will be initiated.

Where complaints are unresolved details of the Complaints Procedure will be provided by the Practice to the applicant.

Complainants will be informed of their right to contact the Information Commissioner for a review of the subject access provision.

14. Fees

Subject Access Requests shall be free of charge for the data subject and, where applicable, for the Data Protection Officer.

Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Practice may charge a reasonable fee based on administrative costs or refuse to act on the request. The Practice shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

[1] UK GDPR see http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

15. Dissemination and Implementation

This Policy may be made available to the Public through the Practice Internet site, in supporting documentation and upon application.

This Policy will be made available to staff through the Practice Intranet site r shared folder system and will be included in training sessions

Leaflets will be available to the Public and to members of staff, in Practice premises which will explain the subject access process.

New employees will be made aware of this policy through the Induction process

The Practice will ensure that processes are in place to implement this policy.

16. Monitoring Compliance with Effectiveness

Compliance with this Policy will be monitored through the provision of quarterly reports to the Board, and will be escalated to the commissioners of the respective contract.

A log of all subject access requests will be maintained. The effectiveness of the log will be regularly reviewed.

Written procedures will detail the compliance process. The effectiveness of the procedures will be reviewed at regular intervals.

Exemplar template documents will be available to the Public in connection with this policy.

Service user satisfaction spot checks will be carried out to establish the effectiveness of the Access to Health Records processes that support this policy.

This Policy will be monitored through the investigation of any related complaints.

17. Associated documents

This Policy should be read in conjunction with the following Practice Policies:

- Data Protection Policy
- Freedom of Information Policy (if applicable)
- Information Governance Policy
- Records Management & Information Lifecycle Policy
- SARs register (to store SARs)

18. References

- Data Protection Act 2018 (including UK GDPR)
- Access to Health Records Act 1990
- Access to Medical Reports Act 1988

- Department of Health Guidance on Access to Health Records Requests 2010
- Freedom of Information Act 2000
- Mental Health Act
- Mental Capacity Act
- NHS Code of Practice: Records Management 2009

19. Appendix A: Fees

Subject Access Requests shall be free of charge for the data subject and, where applicable, for the Data Protection Officer.

Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the Practice may charge a reasonable fee based on administrative costs or refuse to act on the request. The Practice shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

20. Appendix B: Template application form: Access to records.

Please read the Practices 'Accessing Records' leaflet' as it will explain who should complete this form, the charges that you may be asked to pay and inform you of the proof that we will need to verify your identity.

Section 1: Details of the person whose information is required

Surname		Forename(s)	
Previous Surname			
Date of Birth		Male/female	
Current Address Postcode		Previous Address(s) (with dates) Postcode(s)	
Contact number			

Section 2: Please provide us with as much information in this section as you can to help us find what you need

Service users' medical records	
Staff members requesting access to Personnel records	
Staff member requesting access to Occupational Health records	
NHS number (if known)	

I wish to: -	Tick box
View my record	□
Have copies of my record	□

Signature	Date

Section 3: If you require someone else to act on your behalf please complete this section:

Nomination of a representative
I Mr./Mrs./Ms……..hereby authorise ,Willingham-by-Stow to release the information I am requesting to my personal representative who is:- Mr./Mrs./Ms……..(print name) Details of relationship…… Signed…… Date……..

Section 4: If you are not the person whose details appear in section 1 but have a legitimate right to access the information requested please complete this section:

What is your relationship with the person in section 1: Tick one of the boxes (evidence will be required in all cases)	
I am the parent/have parental responsibility of the child whose details appear in section 1 who is under 16 years of age	□
I am the service user's representative as detailed in section 3	□
The service user is deceased and I am the next of kin/designated personal representative	□
The service user is deceased and I have a claim arising out of the death and I wish to see information relating to my claim	□

Please complete and sign the following declaration			
Surname		Forename(s)	
Address Postcode		Contact number	
Signature		Date	

Please return this form to: Dr Daniel Lane, the Practice Caldicott Guardian
At Willingham-by-Stow