Individual Rights Policy

Vine Medical Centre

01/06/2021

Contents

1. Introduction

This policy and accompanying standard operating procedure (SOP) sets out the approach that all staff will take in responding to requests along with useful guidance and steps to follow when requests are received anywhere within the GP Practice.

2. Scope And Definitions

Scope

It is the responsibility of **All** GP staff to respond to and help process requests under the individual rights set out in data protection legislation as soon as it is received by the GP Practice.

Any personal data in relation to an individual, no matter what format, where or how it is stored by the GP Practice falls into the scope of information that can be requested by individuals (i.e. data subjects). All requests must be reviewed, without delay to see if the request can and should be complied with.

Requests received by third parties in regard to access to a data subjects personal data (e.g. the Police or Home Office) should be handled using the process described within the SOP.

Definitions

Commercially confidential Data/Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the GP Practice or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the GDPR.
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).

Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the GDPR.
'Special Categories' of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life

Abbreviation	**Meaning**
CSU	Commissioning Support Unit
DC	Data Custodian
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPO	Data Protection Officer
FPN	Fair Processing Notification (privacy notice)
GDPR	General Data Protection Regulations
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IT	Information Technology

SCW	South, Central and West CSU
SIRO	Senior Information Risk Owner

3. Details of The Policy and Compliance with the Data Protection Legislation

The General Data Protection Regulation (GDPR) provides rights for individuals which fall into 2 distinct categories. Firstly, where an individual wants to know what (or why) data the GP Practice is processing about them and/or have access to or a copy of that data.

Secondly where an individual wants the GP Practice to make changes to what or how the GP Practice is processing their personal data, or for the GP Practice to pass on their personal data to another party. In these requests, the individual is not requesting access to, or a copy of the data itself.

As this can be a complex area to understand, to ensure local compliance the Practice has prepared a process flowchart which can be found at Appendix B.

3.1 Acknowledging Individual Rights

An individual or their representative can exercise several data subject rights to the GP Practice. These do not confer automatic agreement to the request but will be duly considered by the GP Practice – Appendix A and the SOP contains more in depth detail regarding each of the rights.

These rights include but are not limited to the following:-

- obtain from the GP Practice confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, request access to the personal data (a **Subject Access Request/Right of Access**)
- obtain from the GP Practice without undue delay the rectification of inaccurate or incomplete personal data processed by the GP Practice concerning him or her (**Right to Rectification**)
- obtain from the GP Practice the erasure of personal data concerning him or her in certain circumstances (**Right to Erasure**)
- obtain from the GP Practice restriction of processing of personal data concerning him or her in certain circumstances (**Right to Restriction**)
- receive the personal data concerning him or her, which he or she has provided to the GP Practice, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller in certain circumstances (**Right to Data Portability**)

- object to processing of an individual's personal data in certain circumstances (**Right to Object**)
- not be subject to a decision based solely on automated processing by the GP Practice (**Rights related to automated decision making including profiling**)

It should be noted that there are exemptions to some of these rights and whilst the GP Practice must acknowledge the request, there may be legal grounds for not complying with it. Detailed guidance can be found in the SOP.

3.2 Recognising an Individual's Rights Request

- A request can be made verbally or in writing.
- It can also be made to any part of the organisation and does not have to be to a specific person or contact point.
- A request does not need to mention the phrase containing the right being exercised or the relevant GDPR Article to be a valid request. As long as the individual has clearly described their request; this is valid. The Practice will check with the requester that it has understood their request and request any Identification/authorisation (if required).
- The Practice will record the details of all requests we receive.

The format that an Individual's Rights request is received may differ from request to request. In essence, if an individual writes to the GP Practice or speaks to the GP Practice and asks for access, changes or objections of any kind to the personal data the GP Practice is processing about them (whether perceived or actually processing their data) it should be considered and handled where appropriate as an Individual's Rights request.

GP Staff can also submit a request for access to their personal data to the GP Practice.

3.3 Refusing a Request

If the GP practice considers that a request is 'manifestly unfounded' or excessive it can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request

In either case it will need to justify the decision.

For further information please see the ICOs website:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/

3.4 Charging a Fee

- Individuals rights requests are free of charge however the GP practice may in some circumstances be able to charge a fee such as for repetitive requests
- The Practice should base the reasonable fee on the administrative costs of complying with the request.
- If the Practice decides to charge a fee it will contact the individual promptly and inform them.
- The Practice does not need to comply with the request until it has received the fee.

3.5 Information for Requestors

The GP practice must inform the individual without undue delay and within one month of receipt of the request of the following:

If the GP practice is not taking action:

- the reasons it is not taking action;
- their right to make a complaint to the ICO;
- their ability to seek to enforce a right through a judicial remedy

OR

If the Practice is requesting further information:

- if it is requesting a reasonable fee or
- need additional information to identify the individual
- it needs to extend the response time

OR

The Practice is actioning the request:

- Respond to the request

3.6 Calculating Response Time

Under the Data Protection Legislation, the GP practice has **one** Calendar month to respond to any request. In order to provide clarity to staff in the organisation, the GP practice will calculate the time limit from the day the request is received (whether the day after is a working day or not) until the corresponding date in the next calendar month. However, if the date in the preceding month is at the weekend or on a bank

holiday the next working day will be used as the latest date to provide a response as per national guidance.

For further details on national guidance please visit ICO Individual Rights Guidance.

3.7 Extending the Response Time

The practice can extend the time to respond by a further two months if the request is complex or it has received a number of requests from the individual. The practice will let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- the Practice is requesting proof of identity before considering the request

3.8 Verifying Identity

If the GP practice has doubts about the identity of the person making the request it can ask for more information. However, it is important that it only requests information that is necessary to confirm who they are. The Practice will take into account what data is held, the nature of the data, and what it is being used for.

The Practice will let the individual know without undue delay that it needs more information from them to confirm their identity. The Practice does not need to comply with the request until it has received the additional information.

4. Roles and Responsibilities

Practice Manager

It is the role of the Practice Manager to define this policy taking into account legislative and NHS requirements. The Practice Manager is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Subject Access Request (SAR) Lead

The SAR Lead is responsible for processing Individual Rights requests for the GP practice and ensuring that they are responded to in line with Data Protection Legislation.

Data Protection Officer(s) and the SCW IG team

The Data Protection Officer and SCW IG Team will provide advice and guidance in complex or disputed situations or decisions where required.

All GP Practice Staff

All staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of and comply with the obligations under this policy.

5. Training

All staff are required to complete Information Governance training either using the NHS Data Security Awareness Level 1 modules provided by NHS Digital via the e-LfH platform, or other approved training provider. Bespoke training on Individual's Rights may be provided to GP practices by the SCW IG team where this is included in the relevant service level agreement.

6. Monitoring Compliance and Effectiveness

The application of this policy and the accompanying standard operating procedures will be monitored by the Practice Manager.

7. Review

This document may be reviewed at any time at the request of either staff or management, or in response to new legislation or guidance, but will automatically be reviewed every year.

8. References and Associated Documents

Legislation

The Practice is required to comply with Data Protection Legislation. This includes

- the General Data Protection Regulation (GDPR),
- the Data Protection Act (DPA) 2018,

In addition, consideration must also be given to all applicable Law concerning privacy confidentiality and the processing and sharing of personal data including

- the Human Rights Act 1998,
- the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015,
- the common law duty of confidentiality and
- the Privacy and Electronic Communications (EC Directive) Regulations

Consideration must also be given to the

- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health Records Act 1990

Guidance

- Standard Operating Procedures – Individuals Rights Under the Data Protection Legislation and Access to Health Records Act
- ICO Guidance
- NHS Digital looking after your information
- Dept. of Health and Social Care 2017/18 Data Security and Protection Requirements
- NHS England Confidentiality Policy
- Records management: Code of Practice for Health & Social care
- Confidentiality: NHS Code of Practice - Publications - Inside Government - GOV.UK
- Confidentiality: NHS Code of Practice - supplementary guidance
- GMC guidance for managing and protecting personal information
- NHS Choices Your Health and Care Records

END

Appendix A: The Individual Rights in more detail

The Right to be informed (GDPR Articles 12, 13 and 14)

The GP Practice must provide individuals with information including (but not limited to):

- The purposes for processing personal data,
- The retention periods for that personal data, and
- who it will be shared with

This is called 'privacy information' or 'Fair Processing Information' and the Practice must provide privacy information to individuals at the time it collects personal data from them. If it obtains personal data from other sources, it must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.

How and what information should be provided

The information the Practice provides to people must be

- concise,
- transparent,
- intelligible,
- easily accessible, and
- it must use clear and plain language

The Practice will put the Fair Processing Notice on its website.

The Practice must regularly review, and where necessary, update the privacy information. It must bring any new uses of an individual's personal data to their attention before it starts the processing. A Fair Processing Notification checklist is available which can be used to determine what information the notice must contain.

The Right of Access by the Data Subject (Subject Access Request – GDPR Article 15)

What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

What is an individual entitled to?

Individuals have the right to obtain the following from the GP practice:

- confirmation that it is processing their personal data;
- a copy of their personal data; and

- other supplementary information such as
  - the purposes of processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipient it discloses personal data to;
  - retention period for storing personal data or, where this is not possible, the criteria for determining how long it will be stored ;
  - the existence of their right to request rectification, erasure or restriction or to object to such processing;
  - the right to lodge a complaint with the ICO or another supervisory authority;
  - information about the source of the data, where it was not obtained directly from the individual;
  - the existence of automated decision-making (including profiling); and
  - the safeguards provided if the Practice transfers personal data to a third country or international organisation

Much of this supplementary information is provided in the privacy notice.

What about requests made on behalf of others?

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, the Practice needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney if the individual lacks mental capacity.

What about the records of deceased individuals?

The Data Protection Legislation only relates to living individuals. However requests for access to personal data relating to deceased individuals can also be made under another piece of legislation – the Access to Health Records Act (AHRA) 1990. The same rules apply regarding 'fees' etc. under the GDPR; however requests under the AHRA must be completed within 40 calendar days instead of 1 calendar month. The request must still be logged and actioned without undue delay.

The Right to Rectification (GDPR Article 16 and 19)

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the GDPR (Article 5(1) (d)). However, although the Practice may have already taken steps to ensure that the personal data was accurate when it was obtained; this right imposes a specific obligation to reconsider the accuracy upon request.

What do we need to do?

If the Practice receives a request for rectification it should take reasonable steps to check that the data is accurate and to rectify the data if necessary. It should take into account the arguments and evidence provided by the individual.

The Right to Erasure (GDPR Article 17 and 19)

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which it was originally collected or processed for;
- the Practice is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- the Practice is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the Practice is processing the personal data for direct marketing purposes and the individual objects to that processing;
- the Practice has processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- the Practice has to do it to comply with a legal obligation; or
- the Practice has processed the personal data to offer information society services to a child

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR. For further details about the right to erasure and children's personal data please read the ICO guidance on children's privacy.

Right to Restrict Processing (GDPR Article 18 and 19)

Individuals have the right to request the restriction or suppression of their personal data. When processing is restricted, the Practice is permitted to store the personal data, but not use it.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information the Practice holds or have processed their data. In most cases the Practice will not be required to restrict an individual's personal data indefinitely, but it will need to have the restriction in place for a certain period of time.

The Right to Data Portability (GDPR Article 20)

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

The Right to Object (GDPR Article 21)

An individual has the right to object to

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

Right not to be subject to Automated Decision Making and Profiling (GDPR Article 22)

The GDPR applies to all automated individual decision-making and profiling. Article 22 of the GDPR has additional rules to protect individuals if the Practice is carrying out solely automated decision-making that has legal or similarly significant effects on them. The processing is defined as follows:

- **Automated individual decision-making** (making a decision solely by automated means without any human involvement). Examples include an online decision to

award a loan; or a recruitment aptitude test which uses pre-programmed algorithms and criteria. Automated individual decision-making does not have to involve profiling, although it often will do.

- **Profiling** (automated processing of personal data to evaluate certain things about an individual) and includes any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

END

Appendix B: Process Flow Chart

Being updated to add later

Document Control

This document was created by NHS South Central and West Commissioning Support Unit (SCW) and as such the Intellectual Property Rights of this document belong to SCW.

Document Name	Version	Status	Author
Individual Rights Requests Policy *Primary Care template*	1.0	Published	NHS SCW Information Governance Services
Document objectives:	This document supports Practice staff in compliance with Data Protection legislation, achieving best practice in the area of Information Governance and in meeting the requirements of the Data Security and Protection Toolkit		
Target audience:	All staff		
Monitoring arrangements and indicators:	This document will be monitored by NHS SCW Information Governance Services to ensure any legislative changes that occur before the review date are incorporated.		
Approved and ratified by:	Vanessa Young Practice Manager	Date: 01/06/2021	
Date issued:	01/06/2021		
Date uploaded to Website	01/06/2021		
Review date:	01/06/2023		

Change record

Date	Author	Version	Page	Reason for Change
28.08.2020	SCW	1	All	Review for Website publication