REFINE
SURGICAL
SPECIALIST TREATMENT CENTRE

Rossington House
West Carr Road
Retford
Nottinghamshire
DN22 7SW

"Re-defining the effects of time"

www.refinesurgical.co.uk
01777 711 722

CONTENTS

Updates

05/02/2024	1 Introduction - legal basis changes. Appendix A - table to reflect latest ICO guidance

1.Introduction

This Practice guidance summarises what basis personal data may be collected and processed under the General Data Protection Regulation (GDPR) and what the implications are for an individual's information rights. It will be updated as new codes and guidance are issued by regulators and Government departments in 2017/18,

The data subject (Patient) must be told of all the purposes and the legal basis/bases when personal data is collected. It may be that this needs to be broken down and a different basis used for different purposes under GDPR. It's important we get this right as it has implications for providing information to the individual about how we process their data and for data breaches and enforcement/fines. If you change the legal basis once collected (because circumstances change, or you got it wrong), then the individual(s) must be notified of the change.

The lawful bases are not much different to the current 'conditions for processing personal data' under the Data Protection Act and processing of sensitive data. There is a difference to how **legitimate interests** are considered and extra requirements for **explicit consent. This needs careful consideration for a local authority.**

Definition of personal data

'Personal data' means 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 (e.g. NI, NHS, P/M number for social care), location data, an online identifier (e.g. IP address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

There is also a definition of **special categories** of personal data (referred to as 'sensitive personal data in the Data Protection Act).
This is defined in GDPR as *"*processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

For health and social care note that 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

2. Lawfulness of processing

At least one of the 6 lawful basis listed in Article 6 (1) must apply:

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller – **The clinic applies this Condition for Direct Patient care and Safeguarding**

6(1)(f) – Necessary 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. *(UHL note: this last condition is **not available to processing carried out by public authorities in the performance of their public tasks**.)*

For processing special category data, one of the law basis in Article 9 (2) must also apply:

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement - **The clinic applies this Condition for Safeguarding processing.**

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

9(2)(g) – Processing is necessary for 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

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or 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 – **The clinic applies this Condition for Direct Patient care**

9(2)(i) – Processing is necessary for 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

9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)[1] based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Note: These are subject to further definition in the new Data Protection Bill - see Appendix B. For 9(2)(h), we are waiting for further guidance from NHS Digital/ National Data Guardian of how consent for further sharing beyond direct care may apply or over-ride this Article. Recital 53 also gives further guidance on the Article for health and social care.

3. Consent

The GDPR sets a higher standard for consent, compared with the Data Protection Act, so we need to review whether this is still valid. Consent must be **unambiguous** and **freely given** and involve clear affirmative action and recording of that consent.

Consent may be inappropriate if:

- You would still process their data on a different lawful basis if consent was withdrawn or refused, e.g. Adult/Child Protection
- You asked for consent as a precondition of access to services
- You are in a position of power over the individual - e.g. **employer or public authority**

When requesting consent as the basis:

- Ensure that it is given freely, it's specific and informed, unambiguous and explicit.
- Ensure that there is a method of recording the consent (date, time, method)
- Ensure that there is a process in place for an individual to withdraw consent and that it occurs promptly (along with erasure of data unless there is a legal reason to retain)
- Have a document/system in place enabling you to produce a record of all consents, essentially to demonstrate your compliance.

See the ICO's checklist for consent to see if consent is still applicable.

There are other more appropriate lawful bases for processing personal data for public sector services - see table below.
Note this does not currently take account of 'special categories' - see Article 9 which may further restrict basis.

References taken from ICO's GDPR draft consent guidance and Overview of the GDPR

Lawful basis for data collection and processing under GDPR, including individual's information rights

Appendix A. Table linking Article 6 lawful basis and information rights

Lawful basis	Description	Information rights of the individual					
		Access	Rectification [1]	Erasure [2]	Restrict [3]	Object [4]	Portability
Public task (A6.1e)	Task in the public interest or for your official functions, and the task or function has a clear basis in law	Yes	Yes	No - retention applies	Yes	Yes	No
Compliance with legal obligation (A6.1c)	Required by UK or EU law to process data for a specific purpose	Yes	Yes	No - retention applies	Limited	No	No
Contract with an individual (A6.1b)	Supply goods or services they have requested or under an employment contract	Yes	Yes	Yes - if no longer necessary	Yes	Limited	Yes
Vital interests (A6.1d)	To protect someone's life - ~~data subject or someone else.~~	Yes	Yes	Yes - if no longer necessary	Limited	No	No
Consent (A6.1a)	Documented evidence of consent for the purpose	Yes	Yes	Yes	Yes	No	Yes

1. Third parties where personal data is shared or processed also to be notified and data corrected/made complete
2. Full erase ('right to be forgotten) only fully applies with explicit consent, otherwise retain until end of retention period. Still have right to object or restrict processing.
3. Third parties where personal data is shared or processed also to be notified and processing restricted, inform individual and third parties if restriction is removed. If technically possible the fact that processing has been restricted must be flagged/marked on the personal information.
4. You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse unless compelling legitimate grounds that override individual's rights.

Appendix B. The Data Protection Bill (2018) Proposals

9 (2)The processing meets the requirement in point (b), (h), (i) or (j) of Article 9(2) of the GDPR for authorisation by, or a basis in, the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1 of Schedule 1.

9 (3)The processing meets the requirement in point (g) of Article 9(2) of the GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1.

10 (1)For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out—

(a) by or under the supervision of a health professional or a social work professional, or
(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

Appendix C. Recital 53 - Processing of sensitive data in the health and social sector

Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Appendix D. ICO checklist for consent

- can you answer YES to all of these, IF consent is the legal basis?

Asking for consent

We have checked that consent is the most appropriate lawful basis for processing.
We have made the request for consent prominent and separate from our terms and conditions.
We ask people to positively opt in.
We don't use pre-ticked boxes, or any other type of consent by default.
We use clear, plain language that is easy to understand.
We specify why we want the data and what we're going to do with it.
We give granular options to consent to independent processing operations.
We have named our organisation and any third parties.
We tell individuals they can withdraw their consent.
We ensure that the individual can refuse to consent without detriment.
We don't make consent a precondition of a service.
If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.

Recording consent

We keep a record of when and how we got consent from the individual.
We keep a record of exactly what they were told at the time.

Managing consent

We regularly review consents to check that the relationship, the processing and the purposes have not changed.
We have processes in place to refresh consent at appropriate intervals, including any parental consents.
We consider using privacy dashboards or other preference-management tools as a matter of good practice.
We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
We act on withdrawals of consent as soon as we can.
We don't penalise individuals who wish to withdraw consent.