Information Governance Alliance IGA

THE GENERAL DATA PROTECTION REGULATION: GUIDANCE ON CONSENT

Information Governance Alliance IGA

Contents

1 Introduction

The EU General Data Protection Regulation (GDPR) was approved in 2016 and will become directly applicable as law in the UK from 25th May 2018. The current Data Protection Bill, which will become the Data Protection Act 2018 (DPA18), fills in the gaps in the GDPR, addressing areas in which flexibility and derogations are permitted.

The GDPR will not be directly applicable in the UK post Brexit but the DPA18 will ensure continuity by putting in place the same data protection regime in UK law pre- and post-Brexit, equivalent to that introduced by the GDPR which will continue to be applicable throughout the EU member states.

The Bill does not replicate all the provisions of the GDPR but cross-refers to the relevant provisions as appropriate. When the GDPR and DPA18 come into force, it will therefore be necessary to view the DPA18 and the GDPR side by side in order to see the complete picture of all the data protection legislation. This guidance note only refers to the relevant provisions of the GDPR and will therefore need to be updated to refer to the relevant provisions of all the data protection legislation, once the DPA18 comes into force. The guidance will also be kept up to date in light of any relevant guidance issued from Government and the Information Commissioner's Office (ICO).

The GDPR requires that organisations (controllers) that process personal data demonstrate compliance with its provisions. Part of this involves establishing and publishing a basis for lawful processing, and where relevant, a condition for processing special categories data.

Consent is one of a number of options to meet each of these requirements under the GDPR.

There are a variety of consent practices for the use and disclosure of information in health and social care: from 'implied consent' often assumed as the basis for processing for direct care purposes to explicit consent that is obtained for research purposes. These remain valid for common law requirements and are integral to health and social care practices. However some consent practices do not necessarily meet the requirements of the GDPR and even where they do, consent may not be the preferred legal basis the processing of personal data for GDPR purposes.

In this guidance

The word **must** is used in this document to indicate a legal requirement.

The word **should** is used to indicate that, in particular circumstances, there may exist valid reasons not to follow the guidance, but the full implications must be understood and carefully considered before choosing a different course.

The word **may** is used to indicate a discretionary activity for data controllers. This includes decisions where a permissive legal power is available. Under UK law, data controllers which are public authorities are additionally required to act in accordance with public law principles and to exercise their discretion reasonably and fairly, subject to judicial review, so again such organisations will need to understand the full implications and be able to justify their actions and decisions.

2 Key messages

1) Under the GDPR organisations (controllers) must establish, record and inform subjects about the lawful basis that they are relying on to process personal data.

2) Consent is one way to comply with the GDPR, but it is not the only way, and in many health and social care contexts obtaining GDPR-compliant consent (which is stricter than that required for confidentiality) may not be possible.

3) Health and social care professionals do not need to change consent practices that meet confidentiality requirements where their organisation does not rely on consent as the basis for lawful processing for GDPR purposes.

4) Organisations should consider relying on the alternatives to consent for GDPR purposes.

5) Organisations should consider that different individuals' rights provided by the GDPR are engaged depending on which basis for processing is chosen. Generally individuals have more rights where consent is relied on as the basis for lawful processing under the GDPR.

3 Establishing a lawful basis under the GDPR

As controllers under the GDPR, organisations that process personal data must establish and publish the lawful basis that they are relying on for processing personal data.

The GDPR sets out conditions for lawful processing of personal data (Article 6), and further conditions for processing special categories of personal data (Article 9). These are similar to the conditions in Schedules 2 and 3 of the Data Protection Act 1998 (DPA98), with sensitive personal data now called 'special categories' of personal data. As personal data concerning health is one of the special categories, organisations that process such data must be able to demonstrate that they have met a condition in both Article 6 and Article 9 of the GDPR.

As with the DPA, consent and explicit consent are options for lawful processing of personal data and processing of special categories of personal data under the GDPR respectively. However, as with the DPA they are not preferred over the other available conditions, and there are practical implications should an organisation choose to rely on consent.

Organisations should consider the other conditions available before choosing to rely on consent. This guidance highlights the alternatives. However, it is also important to be aware that, if you are relying on consent, you do not necessarily need to refresh all existing DPA consents for GDPR, where existing consent has been given in line with the GDPR requirements. You will need to be confident that your existing consent requests meet the GDPR standard and that consents are properly documented.

You will also need to put in place compliant mechanisms for individuals to withdraw their consent easily. If your existing DPA consents do not meet the GDPR's requirements, you will either need to seek fresh GDPR-compliant consent, or otherwise identify a different lawful basis for your processing (and ensure continued processing is fair (i.e. that the data subjects rights and freedoms are not undermined through a change in processing)), in order to continue the processing.

Organisations are required by the GDPR to include the legal basis for processing in information provided to patients and service users (previously 'fair processing').

4 Confidentiality requirements are unaffected

The fact that consent may be obtained for confidentiality purposes does not mean that consent must also be the lawful basis applied for the purposes of processing data in compliance with the GDPR. Well established national guidance on confidentiality remains applicable.

GDPR requirements do not affect the common law duty of confidence (confidentiality). Health and social care professionals do not need to change their consent practices in order to comply with the GDPR, unless their organisation chooses to rely on consent as the basis for lawful processing under Article 6, or where relevant explicit consent as the basis for processing special categories of personal data under Article 9.

Although the practice of assuming implied consent for processing data for direct care purposes will not comply with the consent standards under the GDPR, this does not mean that implied consent ceases to be valid for confidentiality purposes.

In limited circumstances where an organisation does implement GDPR-compliant consent, this will definitely meet confidentiality requirements.

5 Consent under the GDPR

In the limited circumstances that consent is the only/most appropriate condition to use as the lawful basis for processing – i.e. none of the other conditions in Articles 6 and 9 apply – organisations will need to consider the practical implications, such as ensuring the consent is valid for GDPR purposes.

The GDPR definition of consent in Article 4(11) requires that:

- consent must be given **by a statement or by a clear affirmative action**, and
- consent must be **freely given, specific, informed and unambiguous.**

Article 7 provides the conditions for consent, including when assessing whether consent is freely given [Article 7(4)]. The GDPR recital provides that **'[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'** , and further that **'…consent should not provide a valid legal ground…where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority'** . With this in mind, consent assumed or obtained in the context of health or care provision is unlikely to establish a lawful basis under the GDPR.

For the processing of special categories of personal data, the Article 9 condition requires that the subject gives explicit consent. The GDPR does not give a definition of explicit consent. The ICO suggests explicit consent must be expressly confirmed and recorded in writing, in a very clear and specific statement. However, for practical purposes there may be little difference between consent and explicit consent under the GDPR.

These requirements set a very high bar. As described above, consent obtained or assumed for reasons of confidentiality may not comply with the standard of consent required under the GDPR.

Furthermore the application of consent as a basis for lawful processing has the following practical implications:

- the requirement to facilitate withdrawal of consent – it must be as easy to withdraw as to give consent
- the requirement that organisations must be able to demonstrate that consent has been obtained
- the availability of the following rights:
  - the right to erasure (where the subject withdraws consent and there is no overriding legitimate grounds to continue processing the data)
  - the right to data portability.

These require the implementation of technical and operational procedures specifically to meet these requirements.

Organisations will need to consider these factors when selecting the most appropriate lawful basis and special categories condition where relevant.

1 Recital 42

2 Recital 43

6 Lawful basis for direct care and administrative purposes

All health and adult social care providers are subject to the statutory duty under section 251B of the Health and Social Care Act 2012 to share information about a patient for their direct care. This duty is subject to both the common law duty of confidence and currently the DPA98 (and in due course the DPA18 and GDPR).

For common law purposes, sharing information for direct care is on the basis of implied consent, which may also cover administrative purposes where the patient has been informed or it is otherwise within their reasonable expectations. Under the GDPR, for processing personal data in the delivery of direct care, and for providers' administrative purposes, the Article 6 condition for lawful processing that is available to all publically funded health and social care organisations in the delivery of their functions is:

6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'

Personal data concerning health are special categories of personal data; the most appropriate Article 9 condition for direct care or administrative purposes is:

9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'

These conditions will also be the most appropriate basis for local administrative purposes such as:

- waiting list management
- performance against national targets
- activity monitoring
- local clinical audit
- production of datasets to submit for commissioning purposes and national collections.

These conditions will also apply where an organisation participates in activities with a statutory basis such as responding to a public health emergency.

See **The General Data Protection Regulation Guidance on lawful processing** for information on safeguarding purposes.

See Appendix 1 for an illustration of confidentiality and the GDPR in direct care and administration.

7 Lawful basis for commissioning and planning purposes

Most national and local flows of personal data in support of commissioning are established as collections by NHS Digital either centrally or for local flows by its Data Services for Commissioners Regional Offices. These information flows do not operate on the basis of consent for confidentiality or data protection purposes.

Where the collection or provision of data is a legal requirement, for example where NHS Digital is directed to collect specified data, and can require specified organisations to provide it, GDPR still needs to be complied with and the appropriate Article 6 condition for NHS Digital and the providers of the data is:

6(1)(c) '…for compliance with a legal obligation…'

Commissioners may receive personal data in support of commissioning where confidentiality is set aside by provisions under the Control of Patient Information Regulations 2002, commonly known as 'section 251 support'. Such support does not remove the need for GDPR compliance.

For GDPR compliance, the most appropriate Article 6 condition for disclosure by NHS Digital and for subsequent processing by commissioners in these circumstances is:

6(1)(e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'

Although there is a move to the use of pseudonymised data for commissioning purposes, this data may constitute personal data under the GDPR, so this condition continues to be applicable.

As for direct care purposes, the most appropriate Article 9 condition for commissioning purposes is:

9(2)(h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'

The commissioning of individually tailored services, or for example the approval of individual funding requests should operate on the basis of consent for confidentiality purposes provided the individual is informed or the sharing is otherwise within their reasonable expectations. Again Article 6(1)(e) is the most appropriate condition for GDPR purposes and common law consent practices do not need to be changed.

The conditions for automated processing such as risk stratification may also be 6(1)(e) and 9(2)(h). However, where such processing could result in a decision that affects an individual, it is important that organisations have in place processes that offer a right to object before such decisions are taken, in accordance with Article 22 (this is separately required where implied consent under common law is being relied upon, or otherwise may be required as a condition for section 251 support).

See Appendix 2 for an illustration of confidentiality and the GDPR in commissioning planning.

8 Lawful basis for research

Research organisations that are public authorities may apply Article 6(1)(e) as their Article 6 condition, and commercial research partners may use:

6(1)(f)'…legitimate interests…except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject…'

The Article 9 condition for research is:

9(2)(j) '…scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or member State law which shall be proportionate…and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject …'

A pre-condition of applying Article 9(2)(j) is that the processing has a basis in UK (or EU) law. This basis will include compliance with the common law duty of confidence, the provisions of DPA18 that relate to research, statistical purposes etc. and other relevant legislation, for example section 251 support.

The Article 89(1) requirement is to implement safeguards, in particular to respect the principle of data minimisation by measures such as pseudonymisation and the use of de-identified data wherever possible.

The application of these conditions does not remove the need for consent or an appropriate legal basis (e.g. section 251 support) that meets confidentiality and ethical requirements.

Please refer to Health Research Authority (HRA) guidance on the GDPR.

See Appendix 3 for an illustration of confidentiality and the GDPR in research.

9 Adults who may lack mental capacity

As with the DPA, the GDPR does not give specific provision for the processing of personal data about adults who may lack capacity.

The Mental Capacity Act 2005 (MCA), elaborated in the Mental Capacity Act Code of Practice provides a statutory framework for people who lack capacity to make decisions for themselves, or who have capacity and want to make preparations for a time when they may lack capacity.[3]

3 https://www.gov.uk/government/publications/mental-capacity-act-code-of-practice

The MCA establishes requirements for the assessment of mental capacity, best interests decisions, and for the appointment of individuals with Lasting Power of Attorney (LPA), or Court Appointed Deputies (CAD) who may make decisions on behalf of an individual who lacks capacity in relation to a particular issue.

The provisions of the MCA are unaffected by the GDPR.

Options 6(1)(a) **consent** and 9(1)(a) **explicit consent** cannot be used to establish the legal basis for processing personal data relating to adults lacking capacity. The subjects will have been assessed as unable to give consent, and therefore to give consent that meets the GDPR definition. However a third party with the legal right to make decisions on behalf of an adult who lacks mental capacity, e.g. a LPA or CAD, can give consent for GDPR purposes.

Organisations should apply the conditions described in section 6 for the processing of personal data about individuals who have been assessed as lacking capacity.

The following alternatives are available in life or death situations, but should not be necessary for health or social care organisations in processing data about adults with capacity.

6(1)(d) '…to protect the vital interests of the data subject or another natural person…'

9(1)(c) '…to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent'

These conditions might apply in a situation where an organisation needs to act to prevent harm being caused by a patient or service user to someone who has no relationship with the organisation.

10 Children's information

The GDPR addresses the issue of whether parental consent is required only in the context of online services. Article 8 prescribes **'Conditions applicable to child's consent in relation to information society services'.** Parental consent is required where such services are offered to a child below a specified age. The default is 16, to be reduced to 13 by the DPA18.

This provision has no applicability beyond the provision of these services and the principle of Gillick competence is unaffected.

Publically funded health and social care online services such as Patient Online are not captured by Article 8 because:

1) They are not provided for remuneration as the definition of information society services requires;
2) Article 8 only applies where the condition for lawful processing under Article 6 is consent.

Furthermore, the GDPR provides interpretation that parental consent '**…should not be necessary in the context of preventative or counselling services offered directly to a child.**'[4]

Organisations should use the conditions for direct care described in section 6 as their lawful bases for the provision of publically funded online services.

A further provision of the GDPR in relation to children's information is that transparency information must be provided '**…using clear and plain language, in particular for any information addressed specifically to a child.**'[5]

11 The right to object

It is important to be aware that where the lawful basis for processing relied upon is Article 6(1)(e) '**…for the performance of a task carried out in the public interest or in the exercise of official authority…**', the right to object under Article 21 applies. Where someone objects, an organisation must not continue to process data unless it can **demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims**.

Where the lawful basis in Article 6(1)(e) above is specifically 'for the performance of a task carried out in the public interest', the right to object will not apply where the data are processed for research or statistical purposes subject to the safeguards in Article 89(1).

As a legal right under the GDPR, the right to object is different from the national data opt-out proposed by the National Data Guardian and the existing ability to record type 1 and type 2 objections, which are policy initiatives. The National Data Opt-out is being introduced in May 2018 for implementation and rolled across the health and care system by 2020. The existing resources will include more information about how the National Data Opt-out is being rolled out as well as how the policy fits with the legal framework.

4 Recital 38
5 Article 12

Appendix 1 – Confidentiality and the GDPR in direct care and administration

NHS Trust	GP Practice	Local Authority Social Services Dept.	Care Home
Care Team **--- common law duty of confidence ---** **Confidential information shared with consent for common law** **(or where there is an overriding public interest or other legal basis)**			
GDPR* 6(1)(e) '... exercise of official authority...' 9(2)(h) '...health or social care...' and for safeguarding 9(2)(b) '...social protection law...'	GDPR* 6(1)(e) '... exercise of official authority...' 9(2)(h) '...health or social care...' and for safeguarding 9(2)(b) '...social protection law...'	GDPR* 6(1)(e) '... exercise of official authority...' 9(2)(h) '...health or social care...' and for safeguarding 9(2)(b) '...social protection law...'	GDPR* 6(1)(e) '... exercise of official authority...' 9(2)(h) '...health or social care...' and for safeguarding 9(2)(b) '...social protection law...'

*Organisations process information relating to criminal convictions and offences will need to reference the appropriate provision in DPA18.

Appendix 2 – Confidentiality and the GDPR in commissioning and planning

Health and Social Care providers	NHS Digital	NHS England	Clinical Commissioning Group
--- common law duty of confidence --- Confidential information provided to NHS Digital with legal mandate under directions and disseminated to commissioners as pseudonymised personal data			
GDPR 6(1)(c) '...legal obligation...' 9(2)(h) '...health or social care...'	GDPR 6(1)(c) '...legal obligation...' 9(2)(h) '...health or social care...'	GDPR 6(1)(e) '... exercise of official authority...' 9(2)(h) '...health or social care...'	GDPR 6(1)(e) '... exercise of official authority...' 9(2)(h) '...health or social care...'

Appendix 3 – Confidentiality and the GDPR in research

Health and Social Care providers	Commercial research partner	Arms' length body	University
Research Partners --- common law duty of confidence --- Confidential information shared with consent or with s251 support			
GDPR 6(1)(e) '... exercise of official authority...' 9(2)(j) '...research purposes...'	GDPR 6(1)(f) '...legitimate interests...' 9(2)(j) '...research purposes...'	GDPR 6(1)(e) '... exercise of official authority...' 9(2)(j) '...research purposes...'	GDPR 6(1)(e) '... exercise of official authority...' 9(2)(j) '...research purposes...'

Sources and further reading

The General Data Protection Regulation – Guidance on the role of the Data Protection Officer (Information Governance Alliance)
https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

The General Data Protection Regulation – Guidance on Accountability and organisational priorities (Information Governance Alliance)
https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

The General Data Protection Regulation – Guidance on lawful processing (Information Governance Alliance)
https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

Overview of the GDPR (Information Commissioner's Office)
https://ico.org.uk/for-organisations/data-protection-reform

Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now (Information Commissioner's Office)
https://ico.org.uk/for-organisations/data-protection-reform

Key areas to consider (Information Commissioner's Office)
https://ico.org.uk/for-organisations/data-protection-reform

National Data Opt Out (NHS Digital)
https://www.digital.nhs.uk/national-data-opt-out