Information Governance Alliance

THE GENERAL DATA PROTECTION REGULATION: GUIDANCE ON LAWFUL PROCESSING

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.

This guidance presents the options for establishing lawful processing that are available to health and social care organisations under the GDPR.

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) For health and social care organisations to process personal data, one of the lawful bases for processing data set out in Article 6 must apply.

3) To process special categories of personal data, one of the bases for processing data set out in Article 9 must also apply.

4) To process data relating to criminal convictions and offences, the lawful bases for processing will be set out in the DPA18 as permitted by Article 10.

5) Consent is one way to comply with Article 6 of 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.

6) Organisations should consider relying on the alternatives to consent for GDPR purposes, taking into account 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.

7) Publicly funded health and social care organisations which are public authorities for the purposes of The Freedom of Information Act (FOIA) 2000 will be public authorities for the purposes of the GDPR and they must no longer use 'legitimate interests' as their basis for lawful processing – in the performance of their tasks.

8) The most appropriate basis for lawful processing that is available to publically funded and/or statutory 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…'

9) There are a number of lawful bases for processing special categories of personal data that may be available to health and social care organisations, as set out in Article 9 of the GDPR. The DPA18 will make further provision in respect of these lawful bases for processing special categories of personal data.

3 Context: the legal framework in UK law

It is important to understand the context in the UK because the many of the conditions for lawful processing under the GDPR require a basis in UK law. The DPA18 will provide further clarity on this.

The legal framework that underpins the lawful processing of personal data comprises both legislation and common law:

- for public bodies established by statute, a power to act derived from statute
- for organisations (controllers) – compliance with data protection (GDPR/DPA18) and other legislation
- for organisations and employees – compliance with the common law duty of confidence.

Health and social care services are commissioned, provided, monitored and regulated by organisations that fall in to three broad categories:

- public bodies established by statute, for example:
  - providers: NHS Trusts; NHS Foundation Trusts; Local Authorities
  - commissioners: Clinical Commissioning Groups (CCGs); NHS England; Local Authorities
  - arm's length bodies: NHS Improvement (legally Monitor and Trust Development Authority (TDA)); Care Quality Commission (CQC); National Institute for Health and Care Excellence (NICE); NHS Digital
- non-statutory public bodies, for example:
  - Department of Health (which Public Health England (PHE) and Medicines and Healthcare products Regulatory Agency (MHRA) are legally part of)
- non-statutory organisations include for example:
  - primary care contractors: general practices; pharmacists; opticians; dentists
  - GPs, pharmacists etc. are also considered public authorities under the new data protection regulation.[1]
  - care homes

Public bodies established by statute may only act within their statutory powers otherwise they may be subject to legal challenge for acting ultra vires (outside their powers). They may do things that are reasonably necessary for the performance of their primary functions. However, there is no automatic power to use and disclose personal data unless specifically stated or necessarily implied in legislation. For example, CCGs and NHS England have a duty to commission health services but this does not confer an automatic power to process personal data for their commissioning purposes.

In relation to the use and disclosure of confidential information, powers of public bodies can either be **express** or **implied** and **mandatory** or **permissive**. Generally statutory powers should expressly set aside the duty of confidence, but there may be cases like local authorities, for example, who have implied powers to share information for safeguarding purposes (see section 9).

1 https://ico.org.uk/for-organisations/health/health-gdpr-faqs/

Generally statutory duties to share will override the common law duty of confidence, for example NHS Digital has a mandatory power, to require the provision of information when acting under directions from NHS England or the Secretary of State (see section 6).

All organisations that process personal data must comply with the GDPR and with the DPA18 once the GDPR comes into force. They must also comply with common law requirements including the duty of confidence.

Respecting confidentiality is a key safeguard in protecting the rights, freedoms and interests of data subjects that are referred to in many of the GDPR conditions that are applicable in health and social care contexts. Organisations must have robust and demonstrable measures in place to ensure that its employees respect confidentiality in order to achieve GDPR compliance.

The common law duty of confidence (confidentiality) is not absolute and the courts have recognised three broad circumstances under which confidential information may be disclosed:

- consent – whether express of implied (implied consent means that the subject knows or would reasonably expect the proposed use or disclosure and has not objected)
- authorised or required by law, for example under statute, common law (including duty of care) or legal proceedings.
- Overriding public interest, for example where a patient is contagious or the public is at risk, such that there is a public interest in disclosure that overrides the public interest in maintaining confidentiality.

Please refer to **The General Data Protection Regulation – Guidance on consent for information on the GDPR consent** as a lawful basis and how this interacts with confidentiality requirements.

The GDPR makes specific provisions for **public authorities**. The Data Protection Bill defines organisations that are public authorities under the FOIA as public authorities for the purposes of the GDPR and DPA18. The definition covers more than statutory public bodies including for example, GP Practices and the other non-statutory organisations listed above.

Under the GDPR, public authorities must appoint a Data Protection Officer[2] (DPO) and **legitimate interests** is not available to them as a basis for lawful processing in the performance of their tasks.

2 See the General Data Protection Regulation – guidance on the role of the Data Protection Officer (IGA)

4 Establishing a lawful basis under the GDPR

Conditions for processing

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.

The DPA18 will make further provision in respect of the lawful bases for processing special categories of personal data. It will also include provisions for data relating to criminal convictions and offences where the processing of such data is carried out by organisations other than law enforcement agencies.

Establishing a lawful basis – Article 6

An important change is that legitimate interests (Art. 6(1)(f)) is no longer available to public authorities as a basis for processing in the performance of their tasks.

Health and social care organisations will need to apply another basis for their processing, typically:

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

Relying on this lawful basis requires that:

1) it is necessary for the controller to process the personal data for those purposes (i.e. it is reasonable, proportionate and you cannot achieve your objective by some other reasonable means); and
2) the controller can point to a clear and foreseeable legal basis for that purpose under UK law (whether in statute or common law).

The legal basis does not need to refer specifically to the processing of personal data but must establish the 'official authority' to conduct the activity for which the processing is necessary.

Some examples are given below:

ORGANISATION (TYPE)	SOURCE OF 'OFFICIAL AUTHORITY'
NHS England	NHS Act 2006
Clinical Commissioning Groups	NHS Act 2006
NHS Digital	Health and Social Care Act 2012
GP Practices	NHS England's powers to commission health services under the NHS Act 2006 or to delegate such powers to CCGs.
NHS Trusts	National Health Service and Community Care Act 1990
NHS Foundation Trusts	Health and Social Care (Community Health and Standards) Act 2003
Local authorities	Local Government Act 1974 Children Act 1989 Children Act 2004 Care Act 2014

Although (6)(1)(a) consent is an alternative, in many health and social care contexts obtaining GDPR-compliant consent will not be possible and there are other implications of using consent as a basis. Please refer to **The General Data Protection Regulation Guidance on consent for further information**.

Alternative conditions that may be applicable where 6(1)(e) is not available are:

6(1)(c) '...necessary for compliance with a legal obligation to which the controller is subject or:

6(1)(d) '...necessary in order to protect the vital interests of the data subject or of another natural person'

6(1)(c) may be the appropriate basis for the submission and collection of commissioning and other datasets by providers to NHS Digital. See section 6.

6(1)(d) is available in life or death situations but should not be necessary for health or social care organisations to use in the performance of its tasks. This 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.

Public authorities may be able to use 6(1)(f) **legitimate interests** as a basis for processing carried out not in the performance of their official tasks – for example, the management of a car park permit database or system backup and recovery processes.

Special categories – Article 9

Article 9 lists special categories of personal data and lists conditions that are available to enable the lawful processing of this data. Special categories are similar to sensitive personal data under the DPA, with the conditions having equivalent function to those of Schedule 3 of the DPA.

Genetic data and biometric data are added to the list of special categories although no additional conditions apply to these categories. Data concerning health has a more specific definition than that of the DPA:

'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' (Art. 4(15))

As with the DPA explicit consent (9(2)(a)) is one of the available conditions for processing special categories of data. The GDPR does not define explicit consent but for practical purposes there may be little difference between consent and explicit consent under the GDPR given the high threshold for valid consent under the GDPR and other implications when consent is used. Please refer to The General Data Protection Regulation Guidance on consent for further information.

Sections 5 – 10 of this guidance identify recommended Article 9 conditions for principal health and social care functions.

Criminal convictions and offences – Article 10

Data relating to criminal convictions and offences is not a special category under the GDPR. However the DPA18 will include provisions that meet the requirements of Article 10 and will provide a basis for processing this data where necessary in health and social care contexts.

Organisations that process personal data relating to criminal convictions or offences must establish a basis for this processing with reference to these provisions in DPA18.

The requirement for transparency

A new requirement of the GDPR is the principle of 'accountability' which requires that organisations must be able to demonstrate compliance. Part of this involves transparency and the provision of information to subjects – previously referred to as fair processing.

A specific requirement of the GDPR is that organisations must include their lawful basis for processing information provided to patients, service users and staff (Arts. 13 and 14).

5 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 the processing of personal data in the delivery of direct care (i.e. GPs, dentists, optometrists etc.) and for providers' administrative purposes, the Article 6 condition for lawful processing that is available to all publically funded health and/or statutory 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 section 7 for safeguarding.

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

6 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 (DSCRO). 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'. This 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 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.

7 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 alternative 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.

8 Lawful basis for regulatory and public health functions

Where the processing is necessary for the exercise of a mandated regulatory function, the most appropriate Article 6 and 9 conditions are:

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

9(2)(j) ' …necessary for reasons of public interest in the area of public health…or ensuring high standards of quality and safety of health care and of medicinal products or medical devices…'

As information relating to criminal convictions and offences are not special categories data, organisations will need to reference the Article 10 provisions of DPA18 as a basis for processing of such data for public health or regulatory purposes.

9 Lawful basis for safeguarding

For the purposes of safeguarding children and vulnerable adults, the following Article 6 and 9 conditions may apply:

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

9(2)(b) '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law..'

in particular social protection law.[3]

As information relating to criminal convictions and offences are not special categories data, organisations will need to reference the Article 10 provisions of the DPA18 as a basis for processing of such data for safeguarding purposes.

To meet the requirement in Article 9(2)(b) that the processing is necessary for the purposes of carrying out the obligations of the controller or data subject in the field of social protection law, the provisions of the Children Acts 1989 and 2004, and the Care Act 2014 are relevant.

The Children Act 1989 (CA) establishes implied powers for local authorities to share information to safeguard children. Local authorities have a duty to investigate where a child is the subject of an emergency protection order, is in police protection or where there is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm.

The CA also requires local authorities **'to safeguard and promote the welfare of children within their area who are in need'**[4] and to request help from specified authorities including NHS Trusts and Foundation Trusts, NHS England and CCGs. These are required by the CA to comply **'…with the request if it is compatible with their own statutory or other duties and obligations and does not unduly prejudice the discharge of any of their functions.'**[5] Under the Children Act 2004 local authorities must make arrangements to promote cooperation with relevant partners and others, to improve well-being.[6]

3 Social protection is defined in s. 2(b) of REGULATION (EC) No 458/2007 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 April 2007 on the European system of integrated social protection statistics (ESSPROS)

4 Children Act 1989 s. 17

5 Ibid s. 27

6 Children Act 2004, s. 10

The Care Act 2014 sets out a clear legal framework for how local authorities and other parts of the system should protect adults at risk of abuse or neglect. Local authorities have a duty to make enquiries where an adult is experiencing or is at risk of experiencing abuse or neglect[7], and has duties to collaborate with partners generally and in specific cases.[8]

It remains the responsibility of organisations and the professionals they employ to ensure that they have a basis for processing that meets common law requirements and the requirements of the GDPR; and for public bodies that they are acting within their powers.

10 Lawful basis for employment purposes

For employment purposes, the following condition for lawful processing will apply:

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

For necessary processing of special categories, e.g. health data for employment purposes the following condition will apply:

9(2)(b) '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment…social protection law in so far as it is authorised by Union or Member State law..'

As information relating to criminal convictions and offences are not special categories data. Organisations will need to reference the Article 10 provisions of DPA18 and for example, the provisions of the Safeguarding Vulnerable Groups Act 2006[9] as a basis for Disclosure and Barring Service (DBS) checks and other processing of such data.

7 Care Act 2014 s. 42

8 Ibid ss. 6, 7

9 s. 34ZA inserted by the Protection of Freedoms Act 2012 s. 73

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