NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Changes to data protection legislation (General Data Protection Regulation - GDPR) and legal basis for processing data 2018

Key points:

- The General Data Protection Regulation (GDPR) requires a legal basis for processing personal data. Whilst GDPR provides many more conditions for processing than the Data Protection Act 1998, it is less prescriptive as to how those conditions are met. For the purposes of this document, relevant provisions are:
    - Organisations must have a legal basis for processing personal data.
    - Individuals have a right to be informed about processing of their personal data, and should be given choice over processing wherever possible (consent processes).

- The UK's third generation of data protection law received the Royal Assent and its main provisions commenced on 25 May 2018. The aim of the new Data Protection Act 2018 is to modernise data protection laws to ensure they are effective in the years to come. This paper will refer to the Act as 'data protection legislation' hereafter.

- Consent is only one of the legal bases for processing of personal information. Organisations, particularly public authorities or other providers of publicly funded services, may be legally obliged to process personal data by legislation other than data protection, which means that consent cannot apply, and should not be sought.

- Organisational boundaries in a patient care pathway do not create a barrier to care so long as previously established principles are applied – the Caldicott 'Minimum Necessary' principle is in data protection legislation as a 'data minimisation' principle.

- National and regional systems for shared care records and recording consent for non-care use of data (research, national audit, etc) are under development and public bodies will need to keep this under consideration

- Unless there is a risk of harm to the patient or third party, organisations should always inform them about what is being processed, even if consent is not the legal basis for processing.

- Data Protection Impact Assessments (DPIAs), formerly known as Privacy Impact Assessments (PIAs), provide the evidence for compliance with data protection principles and ethical use of information with respect to individuals' privacy.

- GDPR is grounded in "reasonableness" – document rationales and decision-making processes as applicable to circumstances.

This document contains a few examples of which legal basis will apply in common processing scenarios. These are not comprehensive. The intention is to provide a direction to project managers who may not be data protection subject matter experts, and support

Adapted from guidance produced by Sandre Jones, IG Consultant
April 2018 (Updated July 2018)

them with definition of legal bases for processing in Data Protection Impact Assessments and privacy notice information.

Common Processing Scenarios

Legal basis: patients

GDPR[1] Articles 6 (lawfulness of processing any personal data) and 9 (lawfulness of processing sensitive personal data): particularly

6(1)(c) necessary for legal obligations

6(1)(e) public interest or public duty

6(3) the above supported by Member State law (*UK legislation as applicable to circumstances*)

9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc)

9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity).

9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities.

9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research.

Consent, OR other relevant legislation gives "the rest" of the legal basis for processing:

- Health and safety, patient safety, safeguarding and public health: as applicable to circumstances. Examples: various Children Acts ('s47' is in the 1989 Children Act); Mental Capacity Act 2005 (and associated Deprivation of Liberty Safeguards) and many others – CQC has a useful list here: http://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulations-service-providers-managers-relevant

- Health & Social Care (Safety & Quality) Act 2015 s3 brings the Caldicott 'Duty to share for care' (Principle 7) into law. Providers are required to share information in the best interests of patients and this legislation makes that explicit. Patients who decide to 'opt out' must have potential consequences on the quality of their care fully explained to them

- Health & Social Care Act (2012). Various parts of this legislation directly apply to some organisations (local authorities re: public health, Clinical Commissioning Groups. Part 1, section 2 places a duty on the Secretary of State for Health improve quality of services etc.

- Care Act (2014) provides for integration of health and social care patient/citizen pathways. This legislation includes duty of candour requirements (section 81) for all

[1] https://gdpr-info.eu/ provides an easily navigable unofficial version of GDPR (no endorsement of provider implied/intended). Articles are the law itself; recitals provide context, rationale and clarification and may be relied upon by courts in decision making.

relevant organisations, as well as numerous duties for provision of social care services.

- Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 do not only give the CQC powers. Regulation 2 requires providers to "assess, monitor and improve the quality and safety of the services provided in the carrying on of the regulated activity (including the quality of the experience of service users in receiving those services)" (r2(a))

- GDPR (6)(1)(e) – for service improvement or evaluation or analytics projects, public interest or public duty may be appropriate, with a fully explained rationale for the processing. This is in line with normal 'making a case' practice (business case, audit protocol, other rationale for use of resources documentation).

Remember:
Even where consent is not sought:

- Individuals must be informed appropriately about processing, particularly 'non-care' use and should be given choice where possible, in line with current practice and the common law duty of confidentiality.
- Processing must be demonstrably in the best interests of the individuals, or future populations of individuals; i.e. benefits should not be solely gained by the data controller/processor undertaking the processing or other organisation/body.

See Data Protection Impact Assessment, below, and additional information about research at the Health Research Authority's website[2]. Although overall governance differs, principles of data protection and confidentiality are similar for research and audit.

Legal basis: staff

GDPR Articles 6 (lawfulness of processing any personal data) and 9 (lawfulness of processing sensitive personal data): particularly

6(1)(c) necessary for legal obligations

6(3) the above supported by Member State law

9(2)(b) employment provisions (see also Article 88)

9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc)

9(2)(h) occupational health provisions

Consent, OR other relevant legislation gives "the rest" of the legal basis for processing:

- Employment and employment-related law: as applicable to circumstances, including occupational health, pensions, provision of IT services and equipment, health and safety, etc.

- Obligations in relation to provision of health services (examples: incident reporting and investigation, staff names in patient records)

[2] https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/

- Obligations in relation to registered professions as provided by registration bodies, or other legislation (examples: Duty of Candour; transparency obligations in relation to declarations of interest, freedom of information, etc.)

- GDPR (6)(1)(e) – public interest or public duty may be appropriate, with a fully explained rationale for the processing, for example, service evaluation for improvement, etc. This is in line with normal 'making a case' practice (business case, audit protocol, other rationale for use of resources documentation)

Staff should be appropriately informed about processing of their personal data through recruitment information, contracts of employment and policies, handbooks, etc.

Legal basis: others

Primarily applicable to Foundation Trust membership, patient engagement and charitable activities.

GDPR lawful basis likely to be:

6(1)(c) necessary for legal obligations

6(3) the above supported by Member State law

Consent, in accordance with Article 7 (demonstrable, fully informed, freely given, can be withdrawn)

Other relevant legislation or 'rules' should be provided where appropriate:

- Legal obligations in relation to public interest, safeguarding and (where applicable) from Monitor, charity and company law as applicable to circumstances.
- Foundation Trust membership: NHS Act (2006) Schedule 7
- Charities legislation (Charities Act 2011 and others). Institute of Fundraising has no regulatory force and guidance should be compared with legislation and mandatory codes of practice.
- Equality Act 2010 and other equalities legislation

Special circumstances: complaints, freedom to speak up ('whistleblowing')

The GDPR focus on individuals' rights actually makes it less restrictive than current legislation in many respects. There is no substantive change to principles of processing personal data for complaints or in relation to raising concerns internally.

GDPR: particularly -

6(1)(c) necessary for legal obligations – as supported by relevant law, codes of practice and regulatory requirements

9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc)

Article 90 – professional secrecy – may apply in some circumstances

Other relevant legislation or 'rules' should be provided where appropriate (duty of candour, etc)

Acting on third party information: if there are patient safety allegations or implications then investigation is covered under the 'vital interests'.

Disclosure of information to third parties where no consent is in place: guidance on disclosing third party information in relation to a subject access request may be useful[3]. In summary, consider what the third party may already legitimately know. For example, if a clinician is aware that a family member has been present at discussions with clinicians about the patient's care, then disclosure in line with 'what they already know' may be appropriate as no breach of privacy will occur.

Under GDPR, more consideration of Gillick competency may be necessary in relation to childrens' rights over their information, for example, competent children wishing to restrict parental access to all or part of their records.

"Legitimate interest"

GDPR Article 6(1)(f):
"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

This provision specifically excludes public authorities, who would likely need to rely on 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.") or other legal basis for processing.

Key principle, as noted in key points, is reasonableness, which could include practicability of seeking consent; methods for informing individuals, etc.

[3] https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf - Subject Access Code of Practice, p15 and p36-8

Data Protection Impact Assessments and Privacy by Design

The European Convention of Human Rights Article 8[4] Right to a private and family life is qualified by the rights and freedoms of others – including organisations who are required to process personal information, or who have a legitimate purpose for doing so.

Privacy by Design and Data Protection Impact Assessment (DPIA) simply give personal information the same importance in business cases and planning as finance, human resources and capital and physical assets. All too often, Information Governance ends up being a barrier because data protection and privacy considerations have not been built in from the design of a project.

It is important that DPIA is seen as a process, rather than 'filling in a template', although certain information is always needed:

- whose data?
- what data, and what are we doing with it?
- why (benefits and risks)?
- how (processes, data security)?
- where (which organisations, more data security)?
- when (frequency of processing – one off, regular? and retention)?

A DPIA can be as short as: "Does this project/change include processing personal data?" – No.

For those familiar with research ethics concepts, DPIAs can be thought of as 'research protocols for not-research projects'.

DPIAs for business change projects or procurement can be useful to identify efficiencies as well as to support compliance.

CCG Data Protection Officer
31 May 2018

[4] Implemented into UK law by the Human Rights Act 1998.