UKMi
UK Medicines Information

Clinical Governance Working Group

DATA PROTECTION AND THE GDPR:

TOP TIPS FOR MEDICINES INFORMATION CENTRES

SUMMARY

- **Only record the data you need.**
- **Only keep the data you need.**
- **Only use it for the purposes you obtained it (and closely connected purposes).**
- **Only keep it for as long as you need it.**
- **Make sure data is accurate and up to date as far as possible.**
- **Keep data in secure locations.**
- **Transfer data by the method least likely to result in data breach.**
- **Make sure your organisation's Data Protection Officer knows what data processing you are doing, and how you are doing it. Keep a record of what you have told them, and when.**
- **Keep a record of any actions you have taken, or are taking, following their instructions.**

BACKGROUND

The General Data Protection Regulation (GDPR) is European Union (EU) legislation that became law in the UK on **25th May 2018**. It adds to, and strengthens, data protection requirements currently in force in the UK under the Data Protection Act 1998 (DPA1998). When the GDPR comes into force, the DPA1998 will be repealed. The current Data Protection Bill will become the Data Protection Act 2018, which adds detail where individual countries in the EU are allowed to make country-specific rules.

The GDPR does not replace the duty of confidentiality; confidentiality rules operate alongside the GDPR.

- Confidentiality is about not allowing the unauthorised disclosure or escape of people's personal data.
- GDPR is about processing and handling data, informing people what you are doing with their data, and allowing people (in some circumstances) to control what you do with it.

WHAT ARE PERSONAL DATA?

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The GDPR defines personal data as:

…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.

This includes: name, NHS/hospital number, address, etc.

The GDPR defines 'processing' as:

… any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The safest way to think about this is:

- If it's about a person and it's possible to identify that person either with the data you're looking at, or that plus other data controlled by the same organisation, it's personal data.
- If you're doing anything at all with it, you're probably processing it. That includes putting it in a drawer and leaving it there (storage) or destroying it (erasure or destruction).

The GDPR applies to both automated personal data and to paper filing systems where personal data are accessible according to specific criteria. This includes:

- Old MI enquiries filed in order of date.
- Personnel files.
- Meeting minutes containing personal data.

Sensitive personal data includes health data, and has additional protections beyond those given to 'ordinary' personal data.

Practice Point:

- **Remember that staff and enquirer data are also protected under the GDPR/DPA, not just patient data.**

See:

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

DATA CONTROLLERS AND DATA PROTECTION OFFICERS

- Your employing organisation is the data controller.
- Your organisation will have a Data Protection Officer.

Data Controllers are responsible for, and must be able to demonstrate compliance with the principles of the GDPR.

Data Controllers must maintain records of their processing activities, which supports accountability and allows the organisation to demonstrate compliance with the GDPR, and supports transparency to data subjects.

Practice point: Make sure that your organisation's data controller is aware of what the MI service does and how it processes data, including the provision of patient helplines and conduction of user surveys, where appropriate.

GROUNDS FOR PROCESSING DATA

If you are processing personal data, you need to be doing it on one of the 'grounds' (reasons) specified in the GDPR. The ones most appropriate for NHS MI services are:

- For basic personal data, Article 6(1)(e): …*in the public interest or the exercise of official authority.*
- For processing special categories (e.g. patient health information), Article 9(2)(h): *...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...*
- For archiving

Article 9(2)(h) will cover not only direct care, but also local clinical audit.

Consent

As healthcare professionals, we are used to the concept of getting consent for everything we do. However, it is preferable that a Medicines Information Centre **does not** use consent as the basis for its data processing if it can be avoided. This is because:

- If you rely on consent for data processing, the data subject has additional rights regarding erasure of data (see below). This is likely to cause problems as MI Centres have legitimate reasons for keeping data (e.g. in case of future litigation, or because it is part of the patient's health record).
- Relying on consent as the ground for processing data when you would process it anyway is 'misleading and unfair' according to the Information Commissioner's Office (ICO). Essentially, if you ask for consent, the person must be able to refuse.

***If you do use consent*,** consent must be:

- Given by a statement or clear affirmative action (not an opt-out).
- Freely given, specific, informed, and unambiguous (for each type of processing you are planning to do – e.g. one consent won't do for enquiry answering and clinical research, you'd have to do a separate consent for each).

If you use consent:

- It must be easy for the subject to withdraw consent.
- The organisation must be able to demonstrate that consent has been obtained.
- The subject has the right to erasure (if consent is withdrawn and there is no overriding legitimate ground for continuing to process the data).
- The right to data portability.

Consequently, if you use consent as a basis for processing data, you will need to ensure that you have processes in place to make sure all of the above happens. This is obviously both extremely difficult to achieve and is undesirable in the case of providing healthcare services.

Practice Points:

- **If you operate a patient helpline, consider formally agreeing with the appropriate level of pharmacy management that this is part of your organisation's core business (i.e.,**

providing healthcare). This helps to clarify that it is not necessary to use 'consent' as a basis for processing personal data with respect to the helpline.

- ***Tell* people you are recording their personal information (for record-keeping and to help answer their enquiry) – don't *ask* them.**

See:

- GDPR: Guidance on lawful processing at https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

COLLECTING, RECORDING AND STORING DATA

The GDPR says that you should:

- Only keep the data you need.
- Process data securely.
- Dispose of data you no longer need.
- Keep data accurate and up to date.
- Incorporate organisational and technical measures to ensure that data is only processed appropriately.

What this means for MI:

- **Consider what data you need in order to do the task at hand.** Collect the data you need, but no more. For instance:
  - It's reasonable to record an enquirer's work phone number and an email address, but probably not their personal mobile phone number *unless* they say it's the best way to get in touch with them.
  - It's reasonable to record a patient's name, date of birth, NHS number etc. But if the question is about crushing zopiclone tablets, it's not necessary to collect liver and renal function test results as it's unlikely you would need them to answer that question. On the other hand, it would be sensible to ask whether the patient has swallowing difficulties or an enteral tube (and what kind) and how long the situation is likely to last.
- **Be careful where you record data.**
  - Use the correct information fields in MiDatabank for personal data.
  - For MI enquiries, preferably work directly into MiDatabank. If this is not possible, ensure that any relevant information is copied onto MiDatabank from scrap/jotting paper, and the paper disposed of appropriately (e.g. by shredding/confidential waste if it contains protected data).
- **Consider who has access to what data.**
  - Data held in a password-protected database such as MiDatabank is relatively secure: unauthorised persons cannot access it, and records cannot be removed.
  - If saving/printing off enquiries from MiDatabank, remove enquirer/patient information if it is not required.
  - If you have personal data stored in other locations, e.g. shared drives or filing cabinets, consider who has access.

- **Consult national and organisational guidelines/policy on data recording and storage, and make sure you have departmental policies/SOPs where appropriate.**
    - National guidance is that MI enquiries on MiDatabank are stored permanently, but enquiries stored on paper should be stored for 8 years (25 years for paediatric, obstetric and mental health enquiries).
    - Your organisation probably has guidance on how long to store internal organisational documents such as minutes of meetings and personnel records.

See:

- For details of timescales for retention of pharmacy records: https://www.sps.nhs.uk/articles/retention-of-pharmacy-records/

SHARING/TRANSMITTING DATA

Moving data around is a relatively high-risk activity for data escape. Think about how secure your channels of communication are.

- Can you use a secure email system, such as NHS.Net?
- Don't leave personal data on answerphones, unless you have agreed this with the owner of the answerphone. Even then, it's best not to – in case you ring the wrong number.
- If sending faxes, is the receiving fax a 'safe haven'?
- If sending information by post, do you know who will open it at the receiving end?
- If using the telephone or giving information in person, who can overhear?

USING DATA

GDPR says (in Article 5) that data should be collected for specified purposes, and not further processed in a manner that is not compatible with the original purpose specified.

However, if you have a new purpose, you may not need to change the basis on which you process data as long as the new purpose is compatible with the old purpose.

- Is there any link between the initial purpose and the new purpose?
- What would the subject reasonably expect you to do with their data?
- What is the nature of the personal data you are using?
- The consequences for subjects of the new processing
- Appropriate safeguards

GDPR states that further processing for the following purposes should be considered compatible lawful processing operations:

- Archiving in the public interest
- Scientific research
- Statistical purposes.

However, even if your new purpose is lawful, you also need to consider whether it is *fair* and *transparent*, and give individuals information about the new purpose.

For MI, this means:

- If you have collected someone's data to answer an enquiry, you should inform them if you are going to use it for something significantly different.
- Enquirer satisfaction surveys are likely to come within your original purpose in collecting the data, provided the survey is not onerous: e.g. short, easy to complete, and not too frequent (e.g. one form per enquirer per year).
- Research is likely to be lawful, but you should inform people if you are going to use their data for research.

See:

- https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf
- To tell the difference between audit and research: http://www.hra-decisiontools.org.uk/research/docs/DefiningResearchTable_Oct2017-1.pdf

TRANSPARENCY AND FAIR PROCESSING

Data subjects have the right to know what data is being collected about them, and how it is being used. The GDPR requires that a privacy notice inform data subjects of:

- The data controller's identity
- The data protection officer's contact details
- The purpose of the processing
- The legal basis for processing
- The categories of personal data concerned
- The potential recipients of personal data
- How long the data will be retained
- A list of the data subject's rights
- Any safeguards that will be used if data is to be transferred to a country outside the EU.

In addition, data subjects must be informed that they can complain to the ICO if they believe there is a problem with how their data is being handled.

Your organisation should display this information on its website, and it would be wise to make sure that all MI staff know where to find it.

****Further detail to come when national guidance is produced.****

SUBJECT RIGHTS

Data subjects have various rights under the GDPR. These are:

- **Confirmation** that their data is being processed,
- **Copies** of that data. In most cases, no fee is chargeable, and the data has to be provided within 1 calendar month, in a commonly-used machine readable format (if so requested).
- **Objection** to processing:
    - On the grounds that processing is likely to cause substantial damage or distress and it is unwarranted.

- The right to object does not apply where the individual has consented to processing, processing is necessary to apply with a legal obligation, or to protect the vital interests of the individual.
- The controller must respect the objection unless they can demonstrate compelling legitimate grounds for processing which override the individual's rights or for establishing, exercising or defending legal rights.
- If the processing is for scientific or historical research or statistical purposes pursuant to Article 89(1), the right to object need not be respected where the processing is necessary for the performance of a task carried out for reasons of public interest.

- **Rectification** of inaccurate data (within 1 calendar month of request).
- **Restriction** of processing where accuracy is contested by the data subject, or the data subject has objected to processing, pending verification of legitimate grounds.
- **Erasure** of data where:
  - The basis for processing is consent *or*
  - The subject objects and there are no overriding legitimate grounds
  - The personal data are no longer necessary for the purposes for which they were collected.
  - The right is *not available* in certain cases, e.g. where condition relied on for processing are 'performance of a task carried out in the public interest…' or 'for reasons of public interest in the area of public health in accordance with Art 9(2)(h) or (i).

Summary: Subject Access Rights According to Basis for Processing Data

Ground for Data Processing	Right to Erasure	Right to Portability	Right to Object
Consent	YES	YES	NO – but subject has right to withdraw consent.
Contract	YES	YES	NO
Legal Obligation	NO	NO	NO
Legitimate Interests (of controller)	YES	NO	YES
Public Task	NO	NO	YES
Vital Interests (of subject)	YES	NO	NO

See:

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

DATA BREACH

There is now a **legal requirement to notify** the ICO of a data breach within 72 hours, where there is a risk to data subjects (which would include a breach of confidentiality).

There are two levels of fines depending on the type of infringement and severity of the breach:

- Up to 10,000,000 Euros or 2% of total worldwide turnover
- Up to 20,000,000 Euros or 4% of total worldwide turnover

FURTHER INFORMATION

- For further information on how the GDPR affects the NHS: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

LIMITATIONS

- This is a short-form document providing only basic information. It is not intended to be an exhaustive guide to data handling.
- Information that is unlikely to apply to MI services has not been included in the interests of brevity.
- This document is based on information and guidance available at the time of writing. Content may change as further guidance becomes available.

DISCLAIMER

You should always consult local policies and/or guidance. This document is intended to supplement these, not to replace them.

The information and opinion in this document are general information. The information and opinion are not legal advice, and should not be treated as such.

The information is provided without any representations or warranties, either express or implied.

Although we have attempted to ensure that the information and opinion are true, accurate, complete, current and non-misleading, to the best of our ability, we do not warrant that we have succeeded.

You must not rely on this document as an alternative to legal advice from a legal professional.

If you have any specific questions about a legal matter, you should contact your legal services provider.

Nothing in this disclaimer will:

- Limit or exclude any liability for death or personal injury resulting from negligence;
- Limit or exclude any liability for fraud or fraudulent misrepresentation;
- Limit or exclude any liabilities in any way that is not permitted under applicable law.

AUTHOR

Jen Smith MRPharmS, on behalf of the UKMi Clinical Governance Working Group.