General Medical Council

Agenda item:	**10**
Report title:	**Updates to the GMC's confidentiality guidance for doctors**
Report by:	**Fionnula Flannery**, Head of Strategy and Planning, Standards and Ethics Team, Fionnula.flannery@gmc-uk.org, 0207 189 5367 **Thomas Oppé**, Information Governance Manager, Thomas.oppe@gmc-uk.org, 0161 923 6410
Action:	**To note**

Executive summary

The GMC's confidentiality guidance sets out the principles of confidentiality and protection of patient data that all doctors are expected to understand and follow.

The current version of the confidentiality guidance was published in April 2017. Prior to publication, we asked Tim Pitt-Payne QC to advise on the potential future impact from the upcoming General Data Protection Regulation (GDPR). The advice then was that the guidance was broadly compatible but that minor changes would be needed.

We have now updated the guidance to make those changes. There are no substantial changes to the guidance but we have clarified how doctors should approach consent when considering disclosing information in the public interest. We have also updated the legal annex and references to data protection law throughout the guidance.

Further legal advice on the redrafted guidance has reassured us it is consistent with the GDPR.

The current version of the guidance was subject to an extensive consultation process. Given the minor nature of the changes to this version we do not propose running a further consultation. We will however make sure that the changes are communicated to doctors.

Recommendation

The Executive Board is asked to note the updated guidance and approve its publication in time for the GDPR implementation date.

Background

1 The current version of the confidentiality guidance came into effect in April 2017. The guidance is primarily concerned with doctors' individual ethical and legal duties of confidentiality. The guidance aims to be consistent with data protection law but it is not guidance on the law. This will not change with the introduction of the General Data Protection Regulation (GDPR). However it is necessary to update the guidance to be consistent with data protection law, so that doctors can be confident that when they follow GMC guidance they are likely to be acting lawfully.

What does GDPR mean for individual doctors?

2 That depends on whether or not the doctor is a data controller.

- Doctors who work in managed environments (such as hospitals) are not themselves likely to be data controllers for the purpose of data protection law (and therefore not directly bound by GDPR). Our guidance sets the expectation that the doctor will follow the information governance policies and practices where they work.

- Doctors who are data controllers in their own right (e.g. doctors who run their own businesses, such as GP practices and private practices) are under legal and professional obligations to meet their obligations under data protection law. But our guidance does not provide detailed advice on data protection law – instead we direct doctors to the Information Commissioner's Office for authoritative guidance. We will also signpost to guidance given by the NHS, defence bodies and the BMA.

Proposed changes to the guidance

3 The Executive board will be aware of the changes to consent requirements in the GDPR, and the challenges of reconciling the GDPR with the common law duty of confidentiality.

4 We do not expect doctors to have a detailed technical knowledge of the GDPR's consent requirements. Our intention in the guidance is to provide a practical approach and to reassure doctors that they can use patient information for direct care and secondary purposes in a way which complies with the GDPR and the common law. We are therefore making relatively minor changes in the following areas (more detail is at Annex A).

- **Explicit consent:** we have confirmed that our existing definition of explicit consent aligns with the definition in the GDPR.

- **Implied consent:** it is accepted practice to rely on implied consent to share confidential information when certain conditions are met. While this is acceptable under the common law duty of confidentiality, it does not meet the standards of

consent under GDPR. However, alternative conditions for processing will apply. We are therefore providing reassurance that implied consent will remain an acceptable form of consent when the conditions in our guidance are met.

- **Disclosures in the public interest:** it would be unfair and misleading (and therefore incompatible with GDPR) to ask for consent to process information when the data subject has no genuine or free choice in the matter. We have therefore amended the guidance to make clear that doctors should not ask for consent in cases where they have already decided that disclosure is likely to be justified in the public interest. Doctors should still tell the patient about their intention to disclose the information, unless it is not safe or practicable to do so, and consider any objections the patient makes.

- **Legal annex.** We have updated the legal annex, and all references to data protection law in the guidance.

5 We have also taken the opportunity to make some minor textual changes to reflect recommendations made by the Wellcome Trust in relation to the terminology about patient data that makes most sense to patients. Specifically, 'direct care' is not a concept most patients understand, so we are substituting 'own' care where appropriate.

Consultation and legal advice

6 The current version of the guidance was subject to an extensive consultation process and legal advice. The redrafted guidance has been reviewed by Tim Pitt-Payne QC to ensure it is consistent with the GDPR and other legal requirements. The changes we have made to the guidance are relatively minor and will not require any significant practical changes to how doctors use patient information. On that basis it is not necessary to undertake another consultation.

External communications plan and timeline

7 The key message in external communications will be to reassure doctors that there are no significant changes to the professional guidance as a result of GDPR. We plan to use the first anniversary of the confidentiality guidance (25 April) to publicise the amended guidance. We will publish a blog or similar online article explaining the changes and providing some reassurance to doctors about the impact of GDPR. We will also publicise the wide range of existing support materials, and a new interactive flowchart on the website.

8 The GDPR takes effect on 25 May 2018. We intend to publish the guidance in pdf form in advance of this date (before the end of April) to give doctors time to familiarise themselves with the changes to guidance before it comes into effect.

10 - Annex A

General Medical Council

GMC confidentiality guidance and the General Data Protection Regulation (GDPR) – briefing for GMC staff

Key points

- The General Data Protection Regulation (GDPR) (and other laws and regulations that come into effect at the same time, such as the *Data Protection Act 2018*) will come into effect on 25 May 2018. They will replace the *Data Protection Act 1998*.

- As now, doctors who work in managed organisations (such as hospitals) are unlikely to be data controllers in their own right. This means that data protection law does not apply directly to them, but to the organisations they work for. We expect these doctors to follow our guidance and the information governance policies and processes where they work.

- Doctors who are data controllers in their own right (e.g. doctors who run their own businesses, such as GP practices and private practices) are under legal and professional obligations to understand and meet their obligations under data protection law. They will need to assure themselves that they are complying with the law.

- GMC guidance on confidentiality is consistent with data protection law but it is not guidance on the law. This will not change with GDPR.

- We are updating the guidance so that it is consistent with data protection law, and so that doctors can be confident that when they follow GMC guidance they are likely to be acting lawfully. We are also updating the legal annex to give an overview of GDPR.

- But we will need to be careful not to stray outside our expertise by giving doctors advice that we are not qualified to provide. It is outside our remit and expertise to give doctors advice on the law.

What is the GDPR?

The General Data Protection Regulation (GDPR) will come into effect from 25 May 2018 and will govern how data is processed in the EU and the UK. It (and other laws and

regulations that come into effect at the same time, such as the *Data Protection Act 2018*) will replace the *Data Protection Act 1998*.

What does it mean for the GMC?

The GMC is a data controller, and we will be adjusting the way we use and store personal data - which means any information about an identifiable, living person. You can find more information about planned changes to our processes on *Inside Info*.

What does it mean for doctors?

That depends on whether or not the doctor is a data controller.

Doctors who work in managed environments (such as hospitals) are not themselves likely to be data controllers for the purpose of data protection law (and therefore not directly bound by GDPR). The data controller will be the organisation for which the doctor works, and our guidance sets the expectation that the doctor will follow the information governance policies and practices where they work. It also makes clear that this is the mechanism by which doctors will ordinarily meet the requirements of data protection law.

Doctors who are data controllers in their own right (e.g. doctors who run their own businesses, such as GP practices and private practices) are under legal and professional obligations to understand and meet their obligations under data protection law. But our guidance does not provide detailed advice on data protection law – instead we direct doctors to the Information Commissioner's Office for authoritative guidance.

What does GDPR mean for the confidentiality guidance?

Our confidentiality guidance is primarily concerned with doctors' individual ethical and legal duties of confidentiality as established in practice and the common law. The parts of the guidance relating to disclosure of information are therefore structured according to the accepted defences to a breach of the common law duty of confidentiality, which are that:

- the individual consents
- the disclosure is required by law, or is in response to a court order
- the disclosure is justified in the public interest
- the disclosure is of overall benefit to a person who lacks capacity to make a decision (taking into account the mental capacity laws across the UK).

Confidentiality and data protection law are two separate legal frameworks. Data controllers need to be satisfied that they are acting lawfully under both frameworks. But the legal basis for making a disclosure under the common law will not necessarily be the

same as the legal basis for processing under data protection law. This is the case under the *Data Protection Act 1998* and will remain so under GDPR.

For example, in our guidance we say that doctors can rely on implied consent to share information within the healthcare team when certain conditions are met. This is acceptable under the common law duty of confidentiality, but under GDPR implied consent is not likely to be sufficient to share personal data under Article 6 of the GDPR and is not sufficient to share 'special category data' such as health data under Article 9 of the GDPR data (this is known as 'sensitive personal data' under current data protection law). However the GDPR does provide alternative conditions for processing (see the example in the blue box).

This means that there will be times that a data controller is relying on different legal justifications under the two legal frameworks. But it would be unworkable to expect doctors to consider, for every piece of information they process, what the legal basis is under the common law and data protection law. Instead our ambition is that doctors who follow our guidance can be confident that they will be acting in accordance with data protection law without needing to check on every occasion. We therefore make every effort to make sure that the guidance is compatible with data protection law.

An example – implied consent

In the confidentiality guidance we say that doctors may share information within the healthcare team on the basis of implied consent if certain conditions are met. This is fine as far as the common law duty of confidentiality goes. Implied consent is an accepted concept under the common law as long as it is reasonable to assume that the patient would expect the information to be shared.

But implied consent is not sufficient to share sensitive personal information under data protection law. Consent must be *explicit* to be relied upon for the processing of 'special category data' such as health data (and GDPR sets a high standard for consent). If it is not possible or reasonable to seek explicit consent then it will be necessary to find another lawful basis for processing the data.

But that's ok – there are others to choose from. The lawful bases for processing 'special category data' are set out in Article 9 of the GDPR. The condition that permits processing for healthcare purposes is 9(2)(h) which says:

> *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*

This is likely to be the lawful basis under GDPR for sharing healthcare data without explicit consent in the healthcare team. The advice in our guidance will be based on this analysis. Doctors will not need to analyse GDPR for themselves to share information for direct care in line with our guidance (but we will explain it in the legal annex).

So what will change in the guidance?

The changes will be relatively minor, and will be in the following areas.

- **Explicit consent:** we have confirmed that our definition of explicit consent aligns with the definition in the GDPR, which sets a higher standard for consent than current data protection law. Doctors who are relying on consent for confidentiality purposes will not necessarily be relying on consent for data protection purposes. But sometimes they will be relying on explicit consent for both purposes so our guidance should align with the (higher) GDPR standard.

- **Implied consent:** we will make clear that implied consent will not meet the standards of consent under GDPR, but will provide reassurance that different conditions for processing the information will apply. Implied consent will remain an acceptable form of consent for confidentiality purposes.

- **Disclosures in the public interest:** it would be unfair and misleading (and therefore incompatible with GDPR) to ask for consent to process information when the data subject has no genuine or free choice in the matter. This means that doctors should not ask for consent in cases where they have already decided that disclosure is likely to be justified in the public interest. We will amend the guidance to reflect this, but will also say that doctors should still tell the patient about their intention to disclose the information, unless it is not safe or practicable to do so, and consider any objections the patient makes.

- **Legal annex.** In the legal annex we currently give a high level overview of the *Data Protection Act 1998* and how it relates to other laws governing the use of patient information. We are updating this section, and all references to data protection law in the guidance.

- **Record keeping**. There must be clear records to demonstrate consent under GDPR. We will therefore emphasise the importance of keeping a record of decisions to disclose or not disclose information.

Anticipated frequently asked questions

Will we be providing guidance for doctors on the GDPR?

No. We provide guidance on good medical practice for doctors. The purpose of the guidance is to describe what good practice looks like, by setting out the professional values, knowledge, skills and behaviours expected of all doctors working in the UK.

We make every effort to make sure that the guidance is consistent with the law, but it is not guidance on the law. We do not have the expertise or remit to advise doctors on data protection law; instead we direct them to authoritative sources such as the Information Commissioner's Office.

Can the GMC advise doctors who are data controllers what the GDPR will mean for them on the ground?

Not specifically. In the confidentiality guidance legal annex we will give an overview of data protection law (as we do now) but we cannot advise doctors who are data controllers on their legal responsibilities under data protection law. However we can signpost to other organisations that do this:

The Information Commissioner's Office (ICO) provides a range of guidance for data controllers, including '12 steps to take now' and a GDPR checklist: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The ICO also provide resources designed specifically for the health sector: https://ico.org.uk/for-organisations/resources-and-support/health-sector-resources/

The Information Governance Alliance (England) is developing detailed guidance on GDPR for health and social care organisations: https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance

The BMA has produced a guide for GPs on their responsibilities under GDPR: https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-data-controllers

Can GMC advise on what the legal basis would be for disclosing occupational health reports (or any other confidential information) under GDPR?

Not really. We can explain at a high level how the different legal frameworks of confidentiality and data protection law fit together, and that a data controller might rely on different legal justifications under common law and the GDPR for disclosing confidential information.

For example, an occupational health doctor who was also a data controller would almost certainly need to have the patient's consent to disclose a confidential report to the patient's employer in order to avoid a breach of confidence. It would be unusual for such a disclosure to be justified in the public interest or be required by law.

The doctor could also rely on consent under Article 6 of the GDPR and explicit consent under Article 9 of GDPR for the same disclosure. That would be the simplest approach, as the doctor is relying on explicit consent for both common law and GDPR purposes.

But the GDPR sets a higher standard for consent than the DPA and introduces new rights for data subjects, which data controllers would need to take into account. So the doctor might choose to rely on lawful bases other than consent under Articles 6 and 9 of GDPR (read with clauses 9 and Schedule 1 of the *Data Protection Act 2018*) to disclose the report.

That is a decision for the data controller, and is not a matter the GMC can advise on.