General Medical Council

Confidentiality:

draft guidance for consultation

Working with doctors Working for patients

The duties of a doctor registered with the General Medical Council

Patients must be able to trust doctors with their lives and health. To justify that trust you must show respect for human life and make sure your practice meets the standards expected of you in four domains.

Knowledge, skills and performance

- Make the care of your patient your first concern.
- Provide a good standard of practice and care.
  - Keep your professional knowledge and skills up to date.
  - Recognise and work within the limits of your competence.

Safety and quality

- Take prompt action if you think that patient safety, dignity or comfort is being compromised.
- Protect and promote the health of patients and the public.

Communication, partnership and teamwork

- Treat patients as individuals and respect their dignity.
  - Treat patients politely and considerately.
  - Respect patients' right to confidentiality.
- Work in partnership with patients.
  - Listen to, and respond to, their concerns and preferences.
  - Give patients the information they want or need in a way they can understand.
  - Respect patients' right to reach decisions with you about their treatment and care.
  - Support patients in caring for themselves to improve and maintain their health.
- Work with colleagues in the ways that best serve patients' interests.

Maintaining trust

- Be honest and open and act with integrity.
- Never discriminate unfairly against patients or colleagues.
- Never abuse your patients' trust in you or the public's trust in the profession.

You are personally accountable for your professional practice and must always be prepared to justify your decisions and actions.

Contents

About this **guidance**

1 Our core guidance for doctors, *Good medical practice*,* makes clear that patients have a right to expect that their personal information will be held in confidence by their doctors. This guidance sets out the principles of confidentiality and respect for patients' privacy that you are expected to understand and follow.

2 This guidance outlines the framework for considering when to disclose patients' personal information (see paragraphs 14–35) and then applies that framework to three kinds of purpose for which patient information may be used, accessed or disclosed.

- **Direct care purposes** – these are uses of patient information that directly contribute to the diagnosis, care and treatment of an individual.
- **Indirect care purposes** – these are uses of patient information that contribute to the overall delivery of health and social care, but which fall outside the scope of direct care. Examples include health services management, research, epidemiology, public health surveillance, education and training.
- **Non-care purposes** – these are uses of patient information that are not connected to the delivery of health or social care but which serve wider purposes. These include disclosures for public protection reasons and for the administration of justice, and for purposes such as financial audit and insurance or benefits claims.

This guidance also sets out the responsibilities of all doctors for managing and protecting patient information.

3 In this guidance, we use the terms 'you must' and 'you should' in the following ways.

- 'You must' is used for an overriding duty or principle.
- 'You should' is used when we are providing an explanation of how you will meet the overriding duty.
- 'You should' is also used where the duty or principle will not apply in all situations or circumstances, or where there are factors outside your control that affect whether or how you can follow the guidance.

* www.gmc-uk.org/guidance/good_medical_practice.asp.

4 You must use your judgement to apply the principles in this guidance to the situations you face as a doctor, whether or not you hold a licence to practise and whether or not you routinely see patients. If in doubt, you should seek the advice of an experienced colleague, a Caldicott or data guardian[1] or equivalent, or your professional or regulatory body.

5 You must be prepared to explain and justify your decisions and actions. Serious or persistent failure to follow this guidance will put your registration at risk.

Other materials available

6 Further explanatory guidance is available on our website explaining how these principles apply in situations doctors often encounter or find hard to deal with. At the time of publishing this core guidance, we are also publishing explanatory guidance on:

- patients' fitness to drive and reporting concerns to the DVLA or DVA
- disclosing records for financial and administrative purposes
- reporting gunshot and knife wounds
- disclosing information about serious communicable diseases
- disclosing information for employment, insurance and similar purposes
- disclosing information for education, training, and for learning from adverse incidents and near misses
- responding to criticism in the press.

Ethical and legal duties of confidentiality

7 Trust is an essential part of the doctor-patient relationship and confidentiality is central to this. Patients may avoid seeking medical help, or may under-report symptoms, if they think that their personal information will be disclosed* by doctors without consent, or without the chance to have some control over the timing or amount of information shared.

8 Doctors are therefore under both ethical and legal duties to protect patients' personal information from improper disclosure. But appropriate information sharing is an essential part of the provision of safe and effective care. Patients may be put at risk if those who are providing their care do not have access to relevant, accurate and up-to-date information about them.[2]

9 There are also important uses of patient information for purposes other than direct care. Some of these are indirectly related to patient care in that they enable health services to function efficiently and safely. For example, large volumes of patient information are used for indirect care purposes such as medical research, service planning, risk stratification and financial audit. Other uses are not directly related to the provision of healthcare but serve wider public interests, such as disclosures for public protection reasons.

10 Doctors' roles are continuing to evolve and change. Ensuring a legal and ethical basis for using patient information in a complex health and social care environment is likely to be more challenging than in the context of a single doctor-patient relationship. In this guidance, we aim to support individual doctors to meet their professional responsibilities while working within these complex systems.

* In this guidance, 'personal information' means information from which individuals can be identified. 'Disclosure' includes access to patient records, as well as the release of information. See the glossary for more detailed definitions.

The law

11 The law governing the use and disclosure of personal information is complex and you are not expected to be an expert on the law. But you must keep up to date with, and meet, your legal responsibilities.

12 In the legal annex (page 32), we summarise some key elements of the relevant law, including the requirements of the common law, the *Data Protection Act 1998,* and the *Human Rights Act 1998* and other statutes that require or permit the disclosure of patient information. In the guidance itself, we give overarching advice on how to apply ethical and legal principles in practice.

13 In writing this guidance, we have taken into account the relevant law, but our guidance is not a substitute for independent, up-to-date legal advice. If you are unsure about how the law applies in a particular situation, you should consult your defence body or professional association, or seek independent legal advice.

The framework for considering when to disclose personal information

14 You must be satisfied that there is a legal basis for disclosing personal information. You may disclose personal information if:

- the patient consents, whether explicitly or implicitly (see paragraphs 18–21)
- it is in the best interests of a person who lacks the capacity to consent (see paragraphs 67–77)
- it is required by law (see paragraphs 23–26)
- it is approved through a statutory process (see paragraphs 96–99)
- it can be justified in the public interest (see paragraphs 28–34).

15 When disclosing information about a patient, you must:

- use anonymised or de-identified information if practicable and if it will serve the purpose
- be satisfied that the patient:
  - has ready access to information that explains that identifiable information might be disclosed for the sake of their care, or for local clinical audit, and that they can object
  - has not objected
- get the patient's explicit consent if identifiable information is to be disclosed for purposes other than their care, or local clinical audit, unless the disclosure is required by law or can be justified in the public interest or is approved under a statutory process

- keep disclosures to the minimum necessary
- keep up to date with, and follow, all relevant legal requirements, including the common law and data protection law.[3]

16 You must inform patients about disclosures for purposes they would not reasonably expect, or check that they have already received information about such disclosures.

17 When you are satisfied that information should be disclosed, you should act promptly to disclose all relevant information.

Disclosing information with a patient's consent

18 Seeking a patient's consent to disclose information shows respect, and is part of good communication between doctors and patients. Consent may be explicit or implied.

- Explicit (also known as express) consent is given when a patient actively agrees, either orally or in writing, to a particular use or disclosure of information.
- Implied consent refers to circumstances in which it would be reasonable to infer that the patient agrees to the use of the information, even though this has not been directly expressed (see the glossary for a fuller definition and paragraphs 37–40 for guidance on when this might apply).

In either case, consent must be informed and freely given, and the person giving consent must have the capacity to make the decision.

19 Generally, you should ask for a patient's explicit consent before disclosing, or allowing access to, identifiable information for purposes other than their direct care or local clinical audit. Exceptions to this are when the information is required by law, or when it is not practicable to seek consent, for example because:

- the patient does not have capacity to give consent. In such a case you should follow the guidance on disclosures in the best interests of a patient who lacks capacity (see paragraphs 67–75)
- you have reason to believe that seeking consent would put you or others at risk of serious harm
- seeking consent would be likely to undermine the purpose of the disclosure, for example by prejudicing the prevention or detection of serious crime
- action must be taken quickly, for example, in the detection or control of outbreaks of some communicable diseases, and there is insufficient time to contact the patient
- seeking consent is not feasible given the number or age of records, or the likely traceability of patients.

20 If you disclose personal information without consent you must be satisfied that there is another legal basis for the disclosure (see paragraph 14). Even if consent is not required, you should tell patients about disclosures if it is practicable to do so, unless doing so would undermine the purpose (for example, by prejudicing the prevention or detection of serious crime).

21 We give detailed advice on consent in our guidance *Consent: patient and doctors making decisions together*.*

Disclosing information about a patient who lacks the capacity to consent

22 You may disclose personal information if it is in the best interests of a patient who lacks the capacity to consent. You can find more guidance on this at paragraphs 67–75.

Disclosure required by law

23 You must disclose information if it is required by statute, or if you are ordered to do so by a judge or presiding officer of a court (see paragraphs 118–121). Examples of legal requirements to disclose information about patients are given throughout this guidance with a fuller list in the legal annex.

24 You should satisfy yourself that any disclosure is required by law. Laws and regulations sometimes permit, but do not require, the disclosure of personal information in certain circumstances. Examples are the *Data Protection Act 1998* and the *Crime and Disorder Act 1998*, both of which permit disclosure of information to organisations such as the police, local authorities, social services and government bodies but do not override the legal duty of confidentiality.

25 If disclosure is permitted but not required by law, you should satisfy yourself that there is another legal basis for disclosing the information – for example, because the patient has given consent or disclosure is justified in the public interest, or is approved through a statutory process.

26 You should only disclose information that is relevant to the request. Wherever practicable you should tell patients about disclosures, unless that would undermine the purpose (for example, by prejudicing the prevention or detection of serious crime).

Disclosure approved through a statutory process

27 You may disclose personal information without consent if it has been approved through a statutory process, such as that provided by section 251 of the *National Health Service Act 2006*. You should not disclose personal information if the patient has objected. You can find more guidance on this at paragraphs 96–99.

Disclosure in the public interest

28 Confidential medical care is recognised in law as being in the public interest. The fact that people are encouraged to seek advice and treatment benefits society as a whole as well as the individual. But there can be a public interest in disclosing information to protect individuals or society from risks of serious harm, such as from serious communicable diseases or serious crime. It can also be in the public interest to disclose information for other uses that will benefit society over time. For example, research, epidemiology, public health surveillance, health service planning, and education and training can all serve important public interests.

* www.gmc-uk.org/static/documents/content/Consent_-_patients_and_doctors_making_decisions_together-english.pdf

29 Personal information may be disclosed in the public interest, without a patient's consent, and in exceptional cases where a patient has refused consent, if the disclosure serves an important public interest and the benefits to an individual or to society of the disclosure outweigh both the public and the patient's interest in keeping the information confidential. You must weigh the harms that are likely to arise from non-disclosure of information against the possible harm, both to the patient and to the overall trust between doctors and patients, arising from the release of that information.

30 You can find specific guidance on considering disclosures in the public interest for indirect care purposes at paragraphs 100–106 and guidance on disclosures for public protection purposes at paragraphs 122–128.

31 Before considering whether disclosing personal information would be justified, you should seek the patient's consent, if safe and practicable, and consider any reasons given for refusal. You must also be satisfied that:

- identifiable information is necessary for the purpose
- it is not reasonably practicable to anonymise or de-identify it.

32 Where practicable, you should seek advice from a Caldicott or data guardian or similar expert adviser who is not directly connected with the use for which disclosure is being considered. If possible, you should do this without revealing the identity of any patient.

33 If you decide that disclosing the information is justified in the public interest, you should tell the patient what information has been disclosed, to whom and why, unless it is impracticable to do so, for example because doing so would put you or others at risk of serious harm, or would undermine the purpose of the disclosure.

34 You must document in the patient's records your reasons for disclosing information without consent. You must also record any steps you have taken to seek the patient's consent, to inform them about the disclosure, or your reasons for not doing so.

Disclosures prohibited by law

35 Health professionals are required by certain statutes to restrict the disclosure of some types of information. Examples include the *Human Fertilisation and Embryology Act 1990*, *The National Health Service (Venereal Diseases) Regulations 1974*, the *NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000* and the *Gender Recognition Act 2004*. You can find more detail on disclosures prohibited by law in the legal annex.

Direct care uses **and disclosure**

Sharing information for direct care

36 Appropriate information sharing is an essential part of the provision of safe and effective care. Patients may be put at risk if those who provide their care do not have access to relevant, accurate and up-to-date information about them. Multidisciplinary and multi-agency teamwork is also placing increasing emphasis on integrated care and partnership working, and information sharing is central to this. But information must be shared within the framework provided by law and ethics.

Sharing information for direct care on the basis of implied consent

37 The usual basis for sharing information for direct care is the patient's consent, whether that is explicit or implied (see paragraph 18 for definitions).[4]

38 Most patients understand and expect that some information must be shared within the healthcare team to provide their care. You may rely on implied consent to share relevant information with those who provide (or support the provision of) direct care to the patient if all of the following are met:

- you are satisfied that the person accessing or receiving the information is providing or supporting the individual patient's direct care
- information is readily available to patients explaining how their information will be used, and that they have the right to object
- the patient has not objected
- you are satisfied that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect.[5]

39 Information for patients can be provided in leaflets and posters, on websites, and face to face. It should be tailored to patients' identified needs as far as practicable.

40 You should consider whether patients would be surprised to learn about how their personal information is being used, accessed or disclosed on the basis of implied consent. If you suspect that information is being used in ways that patients would not reasonably expect, you should ask for explicit consent.

Patient objections to sharing information for direct care

41 You must respect the wishes of any patient who objects to particular personal information being shared within the healthcare team or with others who provide care, unless disclosure would be justified in the public interest, or is in the best interests of a patient who lacks the capacity to make the decision.

42 You should explain to the patient the potential consequences of a decision not to allow personal information to be shared with others who are providing their care. You should also consider with the patient whether any compromise can be reached. If, after discussion, a patient who has capacity to make the decision still objects to the disclosure of personal information that you are convinced is essential to provide safe care, you should explain that you cannot refer them or otherwise arrange for their treatment without also disclosing that information.

43 You can find further guidance on disclosures in the best interests of adults who lack capacity at paragraphs 67–75.

If a patient cannot be informed

44 Circumstances may arise in which a patient cannot be informed about the disclosure of personal information, for example in a medical emergency. In such cases, you should pass relevant information promptly to those providing the patient's care.

45 If the patient regains the capacity to understand, you should inform them how their personal information was disclosed if it was in a way they would not reasonably expect.

Local clinical audit

46 All doctors in clinical practice have a duty to participate in clinical audit and to contribute to Clinical Outcome Review Programmes.[6] If an audit will be carried out by the team that provided care, or those working to support them, such as clinical audit staff, you may disclose personal information, so long as you are satisfied that the patient:

- has ready access to information that explains that their personal information may be disclosed for local clinical audit, and that they have the right to object
- has not objected.

47 If a patient does object, you should explain why the information is needed and how this may benefit their own and others' care. If it is not possible to provide safe care without disclosing information for audit, you should explain this to the patient and the options open to them.

48 If clinical audit will be carried out, but not by the team that provided care or those who support them, the information should be anonymised or de-identified. If this is not practicable, or if identifiable information is essential to the audit, you should disclose the information only if you have the patient's explicit consent, or another legal basis for disclosing the information (see paragraph 14).

Sharing information with those close to the patient

49 The people close to a patient can play a significant role in supporting, or caring for, the patient and they may want or need information about the patient's diagnosis, treatment or care. You must be considerate to those close to the patient and be sensitive and responsive in giving them information and support, while respecting the patient's right to confidentiality.

Establishing what the patient wants

50 Early discussions about the patient's wishes can help to avoid disclosures that they might object to. Such discussions can also help to avoid misunderstandings with, or causing offence or distress to, anyone the patient would want information to be shared with.

51 You should establish with the patient what information they want you to share, with whom, and in what circumstances. This will be particularly important if the patient has fluctuating or diminished capacity or is likely to lose capacity, even temporarily. You should document the patient's wishes in their records.

Respecting the patient's wishes

52 If a patient wants information to be shared with a particular person or people, you should do so, unless there is a compelling reason for withholding the information.

53 If a patient who has capacity to make the decision refuses permission for information to be shared with a particular person or group of people, it may be appropriate to encourage the patient to reconsider that decision if sharing the information may be beneficial to the patient's care and support. You must, however, respect the patient's wishes, unless disclosure would be justified in the public interest (see paragraphs 28–34).

54 If a patient lacks capacity to make the decision, it is reasonable to assume that the patient would want those closest to them to be kept informed of their general condition and prognosis, unless they indicate (or have previously indicated) otherwise. You can find detailed advice on considering disclosures about patients who lack capacity at paragraphs 67–75.

Listening to those close to the patient

55 You should not refuse to listen to the views or concerns of those who are close to the patient on the grounds of confidentiality. The information they provide might be helpful in your care of the patient.

56 But you will need to consider whether your patient would consider you listening to the views or concerns of others to be a breach of trust, particularly if they have asked you not to listen to specific people. You might also need to share information with a patient that you have received from others – for example, if it has influenced your assessment and treatment of the patient.

57 If someone close to the patient wants to discuss their concerns about the patient's health, you should make it clear to them that, while it is not a breach of confidentiality to listen to their concerns, you cannot guarantee that you will not tell the patient about the conversation.[7] You should also take care not to disclose confidential information unintentionally – for example, by confirming or denying the person's perceptions about the patient's health.

Patients who may be at risk of harm

58 All patients have the right to a confidential medical service. But challenging situations can arise when confidentiality rights must be balanced against duties to protect and promote the health and welfare of patients who may be unable to protect themselves.

Disclosing information about children who may be at risk of harm

59 For general advice on confidentiality when using, accessing or disclosing information about children and young people, see our guidance *0–18 years: guidance for all doctors*.* For specific guidance on confidentiality in the context of child protection, see our guidance *Protecting children and young people: the responsibilities of all doctors*.†

Disclosing information about adults who may be at risk of harm

60 As a general principle, decisions about how best to provide support and protection to adult patients should be taken in partnership with patients, and should focus on empowering patients to make decisions in their own interests. You must support and encourage patients to be involved, as far as they want and are able, in decisions about disclosing their personal information.

Disclosures required by law

61 There are various legal requirements to disclose information about adults who are known or considered to be at risk of, or to have suffered, abuse or neglect.[8]

62 You must disclose information if it is required by law. You should:

- satisfy yourself that there is a legal basis for the disclosure
- only disclose information that is relevant to the request, and only in the way required by the law
- tell patients about such disclosures whenever practicable, unless it would undermine the purpose of the disclosure to do so.

63 You can find general advice about disclosures that are required or permitted by law at paragraphs 23–26.

Disclosing information about a patient who lacks capacity to consent

64 You must work on the presumption that every adult patient has the capacity to make decisions about the disclosure of their personal information. You must not assume that a patient lacks capacity to make a decision solely because of their age, disability, appearance, behaviour, medical condition (including mental illness), their beliefs, their apparent inability to communicate, or the fact that they make a decision that you disagree with.

65 You must assess a patient's capacity to make a particular decision at the time it needs to be made, recognising that fluctuations in a patient's condition may affect their ability to understand, retain or weigh up information, or communicate their wishes.

66 We give detailed advice on assessing a patient's mental capacity in our guidance *Consent: patients and doctors making decisions together*‡ Practical guidance is also given in the *Adults with Incapacity (Scotland) Act 2000* and *Mental Capacity Act 2005* codes of practice. There is currently no specific mental capacity legislation for Northern Ireland.

* www.gmc-uk.org/guidance/ethical_guidance/children_guidance_index.asp.

† www.gmc-uk.org/guidance/ethical_guidance/13257.asp.

‡ www.gmc-uk.org/guidance/ethical_guidance/consent_guidance_index.asp.

Considering the disclosure

67 You may disclose personal information if it is in the best interests of a person who lacks the capacity to consent. When making decisions about whether to disclose information about a patient who lacks capacity, you must:

- make the care of the patient your first concern
- respect the patient's dignity and privacy
- support and encourage the patient to be involved, as far as they want and are able, in decisions about disclosure of their personal information.

68 You must also consider:

- whether the patient's lack of capacity is permanent or temporary and, if temporary, whether the decision to disclose could reasonably wait until they regain capacity
- any evidence of the patient's previously expressed preferences
- the views of anyone the patient asks you to consult, or who has legal authority to make a decision on their behalf, or has been appointed to represent them
- the views of people close to the patient on the patient's preferences, feelings, beliefs and values, and whether they consider the proposed disclosure to be in the patient's best interests
- what you and the rest of the healthcare team know about the patient's wishes, feelings, beliefs and values.

69 You may need to share personal information with a patient's relatives, friends or carers to enable you to assess the patient's best interests. But that does not mean they have a general right of access to the patient's records or to be given irrelevant information about, for example, the patient's past healthcare.

If a patient asks you not to disclose information

70 If a patient asks you not to disclose personal information about their condition or treatment, and you believe that they lack capacity to make that decision, you should try to persuade them to allow an appropriate person to be involved in their care. In some cases, disclosing information will be required or necessary, for example under the provisions of mental health and mental capacity laws (see the legal annex).

71 If the patient still does not want you to disclose information, but you consider that it would be in their best interests, you may disclose relevant information to an appropriate person or authority. In such cases, you should tell the patient before disclosing the information and, if appropriate, seek and carefully consider the views of an advocate or carer. You must document in the patient's records your discussions and the reasons for deciding to disclose the information.

72 You should share relevant information with anyone who is authorised to make decisions on behalf of, or who is appointed to support and represent, a mentally incapacitated patient. This might be a welfare attorney, a court-appointed deputy or guardian, or an independent mental capacity advocate. Information should also be shared with independent mental health advocates in some circumstances.[9]

Disclosing information when a patient who lacks capacity may be at risk of serious harm

73 You must disclose personal information about an adult who may be at risk of serious harm if it is required by law (see paragraphs 61–63).

74 If disclosure is not required by law, you must give information promptly to an appropriate responsible person or authority if you believe that a patient who lacks capacity may be experiencing, or at risk of, neglect or physical, sexual or emotional abuse, or any other kind of serious harm, unless it is not in their best interests to do so.

75 If you believe that it is not in the best interests of the patient to disclose their personal information (and it is not required by law), you should discuss the issues with an experienced colleague. If you decide not to disclose information, you must document in the patient's records your discussions and the reasons for deciding not to disclose. You must be able to justify your decision.

Disclosing information to protect adults who have capacity

The rights of adults who have capacity to make their own decisions

76 As a general principle, adults who have capacity are entitled to make decisions in their own best interests, even if others consider those decisions to be irrational or unwise. You should usually ask for consent before disclosing personal information about a patient if disclosure is not required by law, and it is practicable to do so. You can find examples of when it might not be practicable to ask for consent at paragraph 19.

77 If an adult patient who has capacity to make the decision refuses to consent to information being disclosed that you consider necessary for their protection, you should explore their reasons for this. It may be appropriate to encourage the patient to consent to the disclosure and to warn them of the risks of refusing to consent. You should however usually respect the patient's refusal to consent to disclosure, even if their decision leaves them (but no one else) at risk of death or serious harm[10]

78 You should do your best to give the patient the information and support they need to make decisions in their own interests – for example, by arranging contact with agencies to support people who experience domestic violence. Adults who initially refuse offers of assistance may change their decision over time.

Disclosing information in the public interest

79 Disclosing personal information about a patient without consent may be justified in the public interest if failure to do so may expose others to a risk of death or serious harm. Disclosure may also be justified if it would assist in the prevention, detection or prosecution of serious crime, especially crimes against the person. You can find further guidance on disclosing information for public protection reasons at paragraphs 122–128.

80 In exceptional cases, disclosing personal information without consent may be justified in the public interest even if no one else is at risk of harm. For example, in some circumstances there may be particular duties to protect a patient from self-harm because they are detained in prison, in hospital, or elsewhere.[11] This is an uncertain area of law, however, and you should seek legal advice before disclosing information without consent in such circumstances.

Indirect care uses **and disclosure**

81 There are many important uses of patient information that contribute to the overall delivery of healthcare, but which fall outside the scope of direct care. Examples of indirect care uses include health services management, research, epidemiology, public health surveillance, and education and training.

82 Without patient information the health and social care system would be unable to plan, develop, innovate, conduct research or be publicly accountable for the services it provides. But anonymised or de-identified information will often be sufficient for such purposes and must be used in preference to identifiable patient information wherever possible. When identifiable information is needed, or it is not practicable to remove identifiable information, it will often be possible to get a patient's explicit consent.

Disclosing anonymised or de-identified information

Anonymous information

83 Information is considered to be anonymous when there is little or no risk of an individual being identified, either from the information itself or in combination with other information. You can disclose information that has been effectively anonymised without breaching confidentiality or data protection law.

84 Removing the patient's name, age, address and other personal identifiers may not be enough to anonymise information effectively. You should follow the guidance from the Information Commissioner's Office, *Anonymisation: managing data protection risk code of practice*, or equivalent guidance, or seek expert advice if you have a role in anonymising information.[12]

De-identified information

85 If anonymised information is not adequate to support the activities for which information is required, you should consider whether de-identified information will be sufficient for the purpose.

86 Information is considered to be de-identified if personal identifiers have been removed, but there is still some risk that individuals could be re-identified unless appropriate controls are put in place. An example of de-identified information is information in which individuals' identities have been masked with pseudonyms or coded references, but from which individuals might be identified if details are correlated with information from other sources.

87 If you disclose de-identified information you should be satisfied that appropriate controls are in place to minimise the risks of individual patients being identified. The controls that are required will depend on the risk of re-identification. You should refer to specialist advice or guidance when assessing risk, or considering what level of control is appropriate. The *Anonymisation: managing data protection risk code of practice* from the Information Commissioner's Office gives detailed guidance on assessing the risk of re-identification, and safeguards that can be used to manage the risk.[13]

The process of anonymising or de-identifying information

88 Information may be anonymised or de-identified for indirect care uses by a person who provides (or supports the provision of) direct care to the patient or, if that is not practicable:

- the task of anonymising or de-identifying the information or seeking patients' consent to disclosure can be delegated[14] to someone who is incorporated into the healthcare team to provide or support direct care on a temporary basis and who is bound by legal and contractual obligations of confidentiality
- identifiable information may be processed in a secure and controlled environment that has the capabilities and is otherwise suitable to process the information. You should be satisfied that the processing environment applies sufficient controls to keep the information secure – for example, by meeting a standard for information security equivalent to ISO 27001 or similar.[15] You should also be satisfied that signed contracts or agreements are in place that include controls on how the information will be used, retained and destroyed, as well as restrictions to prevent the re-identification of individuals.

89 You should be satisfied that patients have been given information about how their information may be used – for example, in a fair processing or privacy notice.

Disclosing information for indirect care purposes from which a patient might be identifiable

90 You must be satisfied that there is a legal basis for disclosing personal information.

Disclosures with consent

91 You should usually ask for consent to disclose identifiable information for indirect care uses if it is practicable to do so, and the information is not required by law. When considering whether it is practicable to ask for consent, you should take account of the factors set out in paragraph 19.

92 You can find further advice on consent at paragraphs 18–21 and in our guidance *Consent: patient and doctors making decisions together* and *Consent to research*.*

Disclosures required by law

93 There are various legal requirements to disclose information for indirect care purposes, such as notification of a known or suspected case of certain infectious diseases or when mandated under the *Health and Social Care Act 2012*. See the legal annex for more detail.

94 You must disclose information if it is required by law. You should:

- satisfy yourself that there is a legal basis for the disclosure
- only disclose information that is relevant to the request, and only in the way required by the law
- tell patients about disclosures whenever practicable, unless it would undermine the purpose of the disclosure to do so
- respect patient objections where there is provision to do so.[16]

95 You can find general advice about disclosures that are required or permitted by law at paragraphs 23–26.

Disclosures approved through a statutory process

96 You may disclose identifiable information without consent if the disclosure has been approved through a statutory process such as that provided by section 251 of the *National Health Service Act 2006*. You should not disclose personal information if the patient has objected.

* www.gmc-uk.org/guidance/ethical_guidance/5993.asp.

97 Section 251 of the *National Health Service Act 2006* (which applies only in England and Wales) allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes where it is not possible to use anonymised information and where seeking consent is not practicable.[17]

98 When considering applications for support under section 251, the Confidentiality Advisory Group of the Health Research Authority considers:

- the feasibility of doing the research or other activity with patients' consent or by using anonymised or de-identified information
- whether the use of identifiable information would benefit patients or the public sufficiently to outweigh patients' right to privacy.[18]

99 The Confidentiality Advisory Group will not usually support disclosures to which a patient has objected.

Disclosures in the public interest

100 Where statutory arrangements such as those described in paragraphs 96–99 exist, the scope for justifying disclosure of identifiable information for indirect care purposes in the public interest is likely to be very limited.

101 Personal information may be disclosed in the public interest, without a patient's consent, and in exceptional cases where a patient has refused consent, if the disclosure serves an important public interest and the benefits to an individual or to society of the disclosure outweigh both the public and the patient's interest in keeping the information confidential.

102 If it is not practicable to anonymise or de-identify the information or to seek or obtain patients' consent without unreasonable effort, and the likelihood of distress or harm to patients is negligible, disclosure for an important indirect care purpose may be proportionate. You should respect a patient's objections to disclosure.

103 Before considering whether disclosure of identifiable information without patients' consent may be justified in the public interest, you must be satisfied that it is:

- necessary to use identifiable information
- not reasonably practicable to anonymise or de-identify the information.

In either case, you must be satisfied that it is not practicable to seek consent or that efforts to contact the patient to ask for consent have been unsuccessful.

104 When considering whether the public interest in disclosures for indirect care uses outweighs patients' and the public interest in keeping the information confidential, you must consider:

- the potential harm or distress to patients arising from the disclosure (for example, in terms of their future engagement with treatment and their overall health)
- the potential harm to trust in doctors generally (for example, if it is widely perceived that doctors will readily disclose information about patients without consent)
- the potential harm to others (whether to a specific person or people, or to the public more broadly) if the information is not disclosed
- the potential benefits to an individual or to society arising from the release of the information
- whether the harms can be avoided or benefits gained without intruding into patients' privacy or, if not, what is the least significant intrusion.

105 You must also consider:

- any views expressed by a patient
- the nature of the information to be disclosed
- what the information will be used for
- who will have access to the information
- the confidentiality and security arrangements in place to protect the information from being disclosed more widely.

106 You should seek advice on whether a disclosure may be justified from a Caldicott or data guardian or similar expert adviser who is not directly connected with the use for which disclosure is being considered. An advisory body may also have a role in advising on, or scrutinising, proposed uses of patient information for indirect care purposes.[19]

Ethical approval for research

107 You should only disclose identifiable information for research if the research has been approved by a research ethics committee.

108 If you are applying for ethical approval for research, you should let the research ethics committee know that identifiable information will be disclosed without consent and tell them the legal basis for the disclosure.[20]

Keeping records

109 You must record any decision to disclose identifiable information, along with your reasons and any advice you sought.

Non-care uses **and disclosure**

110 There are many uses of patient information that are not connected to the delivery of health or social care, but which serve wider purposes. These include disclosures for public protection reasons and for the administration of justice, and for purposes such as financial audit and insurance or benefits claims. Anonymised or de-identified information will often be sufficient for such purposes, and must be used in preference to identifiable patient information wherever possible.

Requests for information from employers, insurers, government bodies and others

111 As a rule, you should seek a patient's explicit consent before disclosing identifiable information for purposes other than the provision of their care or local clinical audit, such as financial audit and insurance or benefits claims.[21]

112 Third parties, such as a patient's insurer or employer, or a government department, or an agency assessing a claimant's entitlement to benefits, may ask you for personal information about a patient, either following an examination or from existing records. In these cases, you should:

- be satisfied that the patient has sufficient information about the scope, purpose and likely consequences of the examination and disclosure, and the fact that relevant information cannot be concealed or withheld from a report
- obtain or have seen written consent to the disclosure from the patient or a person properly authorised to act on the patient's behalf. You may accept an assurance from an officer of a government department or agency or a registered health professional acting on their behalf that the patient or a person properly authorised to act on their behalf has consented
- only disclose factual information you can substantiate, presented in an unbiased manner, which is relevant to the request. You should not usually disclose the whole record, although it may be relevant to some benefits paid by government departments and to other assessments of a patient's entitlement to pensions or other health-related benefits
- offer to show your patient, or give them a copy of, any report you write about them for employment or insurance purposes before it is sent, unless:

- they have already indicated they do not wish to see it
- disclosure would be likely to cause serious harm to the patient or anyone else
- disclosure would be likely to reveal information about another person who does not consent.[22, 23]

113 If a patient refuses or withdraws consent, or if it is not practicable to get their consent, you can still disclose information if it is required by law or can be justified in the public interest (see paragraphs 28–34 and 122–128).

114 If the purpose is covered by a regulation made under section 251 of the *National Health Service Act 2006*, you may make disclosures without a patient's consent, although not if the patient has objected (see paragraphs 96–99).

Disclosures required by law

Disclosures required by statute

115 There are various statutory requirements to disclose information for purposes that are not related to healthcare, such as for the prevention of terrorism and the investigation of road accidents. See the legal annex for more detail.

116 You must disclose information if it is required by law. You should:

- satisfy yourself that there is a legal basis for the disclosure
- only disclose information that is relevant to the request, and only in the way required by the law
- tell patients about such disclosures whenever practicable, unless it would undermine the purpose of the disclosure to do so.

117 You can find general advice about disclosures that are required or permitted by law at paragraphs 23–26.

Disclosing information to courts or in connection with litigation

118 The courts, both civil and criminal, have powers to order disclosure of information in various circumstances. You must disclose information if ordered to do so by a judge or presiding officer of a court. You should object to the judge or the presiding officer if attempts are made to compel you to disclose what appears to you to be irrelevant information, such as information about a patient's relative who is not involved in the proceedings. You should also tell the judge or the presiding officer if you think that disclosure of the information might put someone at risk of harm.

119 If disclosure is ordered, and you do not understand the basis for this, you should ask the court or a legal adviser to explain it to you. You should also tell the patient whose information the court has asked for about the order, unless that is not practicable or would undermine the purpose for which disclosure is sought.

120 In Scotland, the system of precognition means there can be limited disclosure of information in advance of a criminal trial, to both the Crown and defence, without the patient's explicit consent. You should cooperate with precognition if asked to by the Crown or defence. The disclosure must be confined solely to the nature of injuries, the patient's mental state, or pre-existing conditions or health, documented by the examining doctor, and their likely causes. If they want further information, either side may apply to the court to take a precognition on oath. If that happens, you will be given advance warning and you should seek legal advice about what you can and cannot disclose.[24]

121 You must not disclose personal information to a third party such as a solicitor, police officer or officer of a court without the patient's explicit consent, unless it is required by law or can be justified in the public interest. You may disclose information to your own legal adviser in order to take their advice.

Disclosures in the public interest

Disclosing information for public protection reasons

122 Disclosing personal information without consent may be justified in the public interest if failure to disclose may expose others to a risk of death or serious harm.

123 Such a situation might arise, for example, if a disclosure would be likely to assist in the prevention, detection or prosecution of serious crime,[25] especially crimes against the person. When victims of violence refuse police assistance, disclosure may still be justified if others remain at risk, for example from someone who is prepared to use weapons, or from domestic violence when children or others may be at risk.

124 Before considering whether disclosure of personal information would be justified in the public interest, you should seek the patient's consent to disclosure if it is safe and practicable to do so and consider any reasons given for refusal.

125 When deciding whether disclosure of information without consent is justified you must consider:

- the potential harm or distress to the patient arising from the disclosure (for example, in terms of their future engagement with treatment and their overall health)
- the potential harm to trust in doctors generally (for example, if it is widely perceived that doctors will readily disclose information about patients without consent)
- the potential harm to others (whether to a specific person or people, or to the public more broadly) if the information is not disclosed
- the potential benefits to an individual or to society arising from the release of the information

- whether the harms can be avoided or benefits gained without intruding into the patient's privacy or, if not, what is the least significant intrusion.

126 Where practicable, you should also seek advice from a Caldicott or data guardian or similar expert adviser who is not directly connected with the use for which disclosure is being considered. If possible, you should do this without revealing the identity of the patient.

127 If a patient's refusal to consent to disclosure leaves others exposed to a risk so serious that it outweighs the patient's and the public interest in maintaining confidentiality, or if it is not practicable or safe to seek the patient's consent, you should disclose the information promptly to an appropriate person or authority. You should inform the patient before disclosing the information, if it is practicable and safe to do so, even if you intend to disclose without their consent.

128 You must cooperate with requests for relevant information about patients who may pose a risk of serious harm to others. For example, you must participate in procedures set up to protect the public from violent and sex offenders, such as multi-agency public protection arrangements (MAPPA) in England, Wales and Scotland and public protection arrangements in Northern Ireland (PPANI).[26]

Disclosing genetic and other shared information

129 Genetic and some other information about your patient might also be information about others with whom the patient shares genetic or other links. The diagnosis of a patient's illness might, for example, point to the certainty or likelihood of the same illness in a blood relative.

130 Most patients will readily share information about their own health with their children and other relatives, particularly if they are told that it might help those relatives to:

- get prophylaxis or other preventative treatments or interventions
- make use of increased surveillance or other investigations
- prepare for potential health problems.[27]

A patient may also have agreed to sharing information as part of the standard consent processes when they accessed clinical genetics services.

131 However, a patient might refuse to consent to the disclosure of information that would benefit others. For example, this might happen if family relationships have broken down, or if their natural children have been adopted. In these circumstances, disclosure might still be justified in the public interest (see paragraphs 28–34 and 122–128). If a patient refuses consent to disclosure, you will need to balance your duty to make the care of your patient your first concern against your duty to help protect the other person from serious harm.

132 If practicable, you should not disclose the patient's identity in contacting and advising others about the risks they face.

Managing and protecting **personal information**

133 Health and care records can include a wide range of material, such as:

- handwritten notes
- electronic records
- correspondence between health professionals
- visual and audio recordings
- laboratory reports
- communications with patients (including texts and emails).

You must keep records that contain personal information about patients, colleagues or others securely, and in line with data protection requirements.

Knowledge of information governance and raising concerns

134 You must develop and maintain an understanding of information governance that is appropriate to your role. You should be familiar with, and follow, the confidentiality, data protection and record management policies and procedures where you work and know where to get advice on these issues. This includes policies on the use of laptops and mobile devices.

135 If you are concerned about the security of personal information in premises or systems provided for your use, you should follow our advice in *Raising and acting on concerns about patient safety*.*

* www.gmc-uk.org/static/documents/content/RAC_guidance_-english.pdf.

Processing information fairly and in line with the *Data Protection Act 1998*

136 The *Data Protection Act 1998* sets out the responsibilities of data controllers[28] when processing personal data as well as a number of rights for individuals (known as data subjects). Doctors will not usually be data controllers in their individual clinical roles, as the data controller will normally be the organisation for which they work. But there are exceptions to this – for example, doctors providing private services or GPs providing NHS services under contract might be data controllers.

137 If you are a data controller you must understand and meet your obligations under the *Data Protection Act 1998* (see the legal annex for more detail). This includes responsibilities to make sure that a patient's personal information is handled in ways that are transparent and in ways that they would reasonably expect. You must make sure that information is readily available to patients that explains:

- who has access to information that might identify them and for what purposes
- their options for restricting access to some or all of their records
- their rights to complain about how their information is processed, and how to make a complaint.

Detailed guidance is available on the website of the Office of the Information Commissioner.[29]

138 Whether or not you are a data controller, you must process patient information fairly. This means that you must be open with patients about how their information will be used, accessed and disclosed, even if there are limitations to the degree of choice the patient is able to exercise. For example, a patient may not be able to determine the design of the system in which their records are held, but if they know how their information will be processed they can decide whether to accept the service on those terms.

139 If a patient objects to the way their personal information is processed, you should try to find an alternative solution if it is practicable to do so. If it is not possible to manage the information differently (for example, because a request undermines the provision of safe care, or because it places unmanageable administrative demands upon the service), then you should make sure that the reasons are explained to the patient.

Improper access and disclosure

140 Many improper disclosures of patient information are unintentional. Conversations in reception areas, at a patient's bedside and in public places may be overheard. Notes and records may be seen by other patients, unauthorised staff, or the public if they are not managed securely. Patient details can be lost if handover lists are misplaced, or when patient notes are in transit.

141 You must make sure that any personal information about patients that you hold or control is effectively protected at all times against improper disclosure. You should not leave patients' records, or other notes you make about patients, either on paper or on screen, unattended. You should not share passwords.

142 You should not share personal information about patients where you can be overheard, for example in a public place or in an internet chat forum. You should follow our guidance *Doctors' use of social media*.*

143 You must not access patients' personal information unless you have a legitimate reason to view it.

Records management and retention

144 Unless you have a relevant management role, you are not expected to assess the security standards of large-scale computer systems provided for your use in the NHS or in other managed healthcare environments.

145 If you are responsible for managing patient records or other patient information, you must make sure that the records you are responsible for are made, stored, transferred, protected and disposed of in line with the *Data Protection Act 1998* and other relevant laws. You should make use of professional expertise when selecting and developing systems to record, access and send electronic data.[30]

146 The UK health departments publish guidance on how long health records should be kept and how they should be disposed of. You should follow the guidance, even if you do not work in the NHS.[31]

147 You must make sure that any other records you are responsible for, including financial, management or human resources records, or records relating to complaints, are kept securely and are clear, accurate and up to date.[32] You should make sure that administrative information, such as names and addresses, can be accessed separately from clinical information so that sensitive information is not displayed automatically.

148 If you are responsible for employment contracts, you must make sure they contain obligations to protect confidentiality and to process information in line with data protection laws. You should make sure that any staff you manage are trained and understand their responsibilities.

The rights of patients to request access to their own records

149 Patients have a right to request access to their own health records, although there are some exceptions to this.[33] You should respect, and help patients to exercise, their legal rights to have access to, or copies of, their health records. The Office of the Information Commissioner gives guidance on what fees you may charge. You should also follow our guidance on fees in *Financial and commercial arrangements and conflicts of interest*.†

Electronic communications with patients

150 Wherever possible, you should give patients information in ways that meet their language and communication needs. Electronic communication, for example by email or text messaging, can be convenient and can support effective communication between doctors and patients.

151 You must however take reasonable steps to make sure that patient information is secure when it is stored or transmitted. You must also be satisfied that the patient has agreed to be contacted electronically.[34]

* www.gmc-uk.org/guidance/ethical_guidance/21186.asp.

† www.gmc-uk.org/guidance/ethical_guidance/21161.asp.

Disclosing information after a patient has died

152 Your duty of confidentiality continues after a patient has died.[35]

153 There are circumstances in which you must disclose relevant information about a patient who has died, for example:

- when disclosure is required by law
- to help a coroner, procurator fiscal or other similar officer with an inquest or fatal accident inquiry[36]
- on death certificates, which you must complete honestly and fully
- when a person has a right of access to records under the *Access to Health Records Act 1990* or the *Access to Health Records (Northern Ireland) Order 1993*, unless an exemption applies (see the legal annex)
- when disclosure is necessary to meet a statutory duty of candour.[37]

154 In other circumstances, whether and what personal information may be disclosed after a patient's death will depend on the facts of the case. If the patient had asked for information to remain confidential, you should usually respect their wishes. If you are unaware of any instructions from the patient, when you are considering requests for information you should take into account:

- whether the disclosure of information is likely to cause distress to, or be of benefit to, the patient's partner or family[38]
- whether the disclosure will also disclose information about the patient's family or anyone else
- whether the information is already public knowledge or can be anonymised or de-identified
- the purpose of the disclosure.

155 Circumstances in which you should usually disclose relevant information about a patient who has died include:

- when disclosure is authorised under section 251 of the *National Health Service Act 2006*, or is justified in the public interest, such as for education or research
- for public health surveillance, in which case the information should be anonymised or de-identified, unless that would defeat the purpose
- for local clinical audit
- when a parent asks for information about the circumstances and causes of a child's death
- when a partner, close relative or friend asks for information about the circumstances of an adult's death, and you have no reason to believe that the patient would have objected to such a disclosure
- when disclosure is necessary to meet a professional duty of candour[39]
- when it is necessary to support the reporting or investigation of adverse incidents, or for Clinical Outcome Review Programmes.[40]

156 Archived records relating to deceased patients remain subject to a duty of confidentiality, although the potential for disclosing information about, or causing distress to, surviving relatives or damaging the public's trust will diminish over time.[41]

Glossary

This glossary defines the terms used in this document. These definitions have no wider or legal significance.

Information

Anonymised information. Information from which there is little or no risk of an individual being identified, either from the information itself or in combination with other information.

De-identified information. Also known as pseudonymised information. Information from which individuals cannot be identified by the recipient, but which enables information about different patients to be distinguished or to enable information about the same patients to be linked over time (for example, to identify drug side effects). A 'key' (which connects the codes to patient identifiers) might be retained by the person or service that coded the information, so it can be reconnected with the patient. Compare with **anonymised information**, above.

Identifiable information. Information from which a patient can be identified. Their name, address and full postcode will identify a patient; combinations of information may also do so, even if their name and address are not included. Information consisting of small numbers and rare conditions might also lead to the identification of an individual. Compare with **anonymised** and **de-identified information**, above.

Personal information. Information about people that doctors learn in a professional capacity and from which individuals can be identified (see also **identifiable information** above).

Consent

Consent. Agreement to an action based on knowledge of what the action involves and its likely consequences.

Explicit consent. Consent that is expressed orally or in writing. Also known as express consent.

Implied consent. Consent that can be inferred if the patient has been informed that information is to be disclosed, the purpose and extent of the disclosure, and that they have a right to object, but have not objected.

Other terms

Clinical audit. Evaluation of clinical performance against standards or through comparative analysis, to inform the management of services.

Direct care. Activities that directly contribute to the diagnosis, care and treatment of an individual.

Disclosure. The provision or passing of information about a patient to anyone other than the patient, regardless of the purpose. Sharing information within healthcare teams is a form of disclosure, as is providing access to patients' records.

Healthcare team. The healthcare team comprises the health and social care professionals who give direct care to a patient, and the administrative and other staff who support the provision of that care. Others who might form part of the healthcare team, but with whom patients might not expect information to be shared, include prescribing advisers who review a patient's medicine needs to improve safety, efficacy and efficiency in doctors' prescribing.

Public interest. The interests of the community as a whole, or a group within the community, or individuals. Paragraphs 28 and 29 give an explanation of the balancing exercise required to decide if disclosure might be justified in the public interest.

Legal annex

There is no overarching statute that governs the disclosure of confidential information. The common law and statutes that require or permit the disclosure of patient information interact in complex ways and it is not possible to decide whether a use or disclosure of patient information would be lawful by considering any aspect of the law in isolation.

This section sets out some of the key elements of the law that are relevant to the use and disclosure of patient information but it is not comprehensive. It is also not intended to be a substitute for independent, up-to-date legal advice. If you are unsure about the legal basis for a request for information, you should ask for clarification from the person making the request and, if necessary, seek independent legal advice.

Sources of legal rights to confidentiality, data protection and privacy

The common law

The common law imposes a duty on doctors to respect the confidentiality of a patient's personal information. This duty is derived from a series of court judgments, which have established the principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances.

It is generally accepted that the common law allows disclosure of confidential information if:

- the patient consents, whether explicitly or implicitly
- it is required by law, or in response to a court order
- it is justified in the public interest.

Data Protection Act 1998

The *Data Protection Act 1998* regulates the processing of personal data about living individuals in the UK. It sets out the responsibilities of data controllers when processing personal data as well as a number of rights for individuals, including rights of access to their information.

The Act is based around eight data protection principles, which state that personal data must:

- be fairly and lawfully processed
- be processed for limited purposes and not in any manner incompatible with those purposes
- be adequate, relevant and not excessive
- be accurate and up to date
- not be kept for longer than is necessary
- be processed in line with the data subject's rights
- be secure
- not be transferred to other countries without adequate protection.

The first principle of the Act states that data must be processed fairly. This means that a patient's personal information must be handled in ways that are transparent and in ways that patients would reasonably expect. Even if there is a legal basis for disclosing patient information without consent (for example, if the disclosure is mandated by law), data controllers should still take reasonable steps to make sure that patients are made aware of:

- the legal requirement to disclose their information
- what data will be disclosed, to whom, how and when
- what rights they have to object, and how to do so
- where to find more information about how their data will be processed.

The processing must also be lawful. The Act permits, but does not require, disclosure of personal data in some circumstances. For example, if a disclosure of information would be a breach of the common law duty of confidentiality, it would also be unlawful under the Act.

One or more of the 'conditions for processing' in Schedules 2 and 3 to the Act must also be met.

- In all cases, at least one of the conditions set out in Schedule 2 must be met.
- Where 'sensitive personal data' are being used at least one of the conditions in Schedule 3 must also be met. Information on a patient's medical record is likely to be 'sensitive personal data' for the purposes of the Act.

In addition, the *Data Protection (Processing of Sensitive Personal Data) Order 2000* sets out other conditions for processing sensitive personal data. These permit processing that is 'in the substantial public interest' and which is necessary for carrying out certain public functions, which include preventing or detecting crime, and protecting the public against malpractice or other seriously improper conduct (for example, through investigation into a healthcare professional's fitness to practise – see below).

The Information Commissioner is the authority responsible for upholding information rights in the UK. Detailed guidance on complying with the Act is available on the website of the Information Commissioner's Office.*

Human Rights Act 1998

The *Human Rights Act 1998* incorporates the *European Convention on Human Rights* (ECHR) into UK law. A person's right to have their privacy respected is protected by Article 8 of the ECHR. This right is not absolute, and may be interfered with where the law permits and where it is *'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*

Any interference with a person's right to privacy must be a necessary and proportionate response to the situation. This means that there must be a fair balancing of competing interests. These include:

- the potential damage caused to the individual whose privacy will be breached
- society's interest in the provision of a confidential health service
- the public interest that will be achieved through breaching the individual's privacy.

* https://ico.org.uk/for-organisations/guide-to-data-protection.

Relevant factors to take into account when considering a disclosure in the public interest are given at paragraphs 28–29, 100–106, and 122–128 of this guidance.

Other ECHR rights that may be relevant to considerations about whether the disclosure of a patient's personal information is necessary and proportionate include Article 2 (which protects the right to life), Article 3 (which prohibits torture or inhumane or degrading treatment or punishment) and potentially others. Such considerations are complex and you should seek legal advice if necessary.

Freedom of Information Act 2000

The *Freedom of Information Act 2000* provides public access to information held by public authorities. Public authorities include government departments, local authorities, the NHS, state schools and police forces. The Act does not give people access to their own personal information such as their health records. If a member of the public wants to see information that a public authority holds about them, they should make a subject access request under the *Data Protection Act 1998*. Guidance about the *Freedom of Information Act 2000* is available on the website of the Information Commissioner's Office.

Computer Misuse Act 1990

It is an offence under this Act to gain unauthorised access to computer material. This would include using another person's ID and password without authority to use, alter or delete data.

* www.cqc.org.uk/file/4201.

Statutes that require, permit or prevent disclosure of patient information

Regulation of healthcare providers and professionals

Various bodies regulating healthcare providers and professionals have legal powers to require the disclosure of information, including personal information about patients. The following sets out only a selection of these bodies, and gives a summary of their most relevant powers and refers to the codes of practice they publish about how they use their powers.

The **Care Quality Commission** (CQC) has powers of inspection and entry and to require documents and information under the *Health and Social Care Act 2008*. Sections 76 to 79 govern the CQC's use and disclosure of confidential personal information. Section 80 requires it to consult on and publish a code of practice on how it obtains, handles, uses and discloses confidential personal information. The code of practice is available on the CQC's website.*

Healthcare Inspectorate Wales has powers under the *Health and Social Care (Community Health and Standards) Act 2003* to access a patient's personal information.

Healthcare Improvement Scotland has similar powers in relation to registered independent healthcare providers under the *Public Services Reform (Scotland) Act 2010*.

The **Regulation and Quality Improvement Authority** has powers under sections 41 and 42 of the *Health and Personal Social Services (Quality, Improvement and Regulation) (Northern Ireland) Order 2003* to enter establishments and agencies and health and social services bodies or providers' premises and inspect and take copies of records, subject to the protection of confidential information provided for in section 43.

The **NHS Counter Fraud Service** has powers under the *National Health Service Act 2006* and the *National Health Service (Wales) Act 2006* to require the production of documents to prevent, detect and prosecute fraud in the NHS. The Department of Health (England) and Welsh Assembly Government have published codes of practice for the use of these powers.

The **General Medical Council** has powers under section 35A of the *Medical Act 1983* (as amended) to require disclosure of information and documentation relevant to the discharge of our fitness to practise functions, provided such disclosure is not prohibited by other laws. Other professional regulators have similar powers. For example the **Nursing and Midwifery Council** has powers to require disclosure of patient information for the purpose of carrying out its fitness to practise functions in some circumstances under section 25 of the *Nursing and Midwifery Order 2001*.

The **Parliamentary and Health Service Ombudsman,** the **Northern Ireland Ombudsman,** the **Public Services Ombudsman for Wales** and the **Scottish Public Services Ombudsman** have legal powers similar to the High Court or Court of Session to require the production of documents and the attendance and examination of witnesses for the purposes of investigations about the health bodies that fall within their remits.

Other Acts that provide for some form of access to personal information about patients

Abortion Regulations 1991 and ***Abortion (Scotland) Regulations 1991.*** A doctor who has carried out a termination of pregnancy must notify the appropriate Chief Medical Officer of that fact within seven days of the termination.

Access to Health Records Act 1990 and ***Access to Health Records (Northern Ireland) Order 1993***. These pieces of legislation provide rights of access to a deceased patient's personal representative and any person who may have a claim arising out of a patient's death. This is not a general right, however, and access should be limited to information of relevance to the claim. Access should be limited or refused if there is evidence that the patient would have expected that the information would not be disclosed to the applicant, if disclosure is likely to cause serious harm to anyone else, or if it would also disclose information about a third party (other than a healthcare professional involved in the deceased person's care) who does not consent. Access must be refused to records that contain a note, made at the patient's request, expressing that they did not wish access to be given on an application under the Act.

Access to Medical Reports Act 1988 and ***Access to Personal Files and Medical Reports (Northern Ireland) Order 1991***. These pieces of legislation give patients the right to see medical reports written about them, for employment or insurance purposes, by a doctor who is or has been responsible for the clinical care of the individual. This includes the right to see reports written by the patient's GP or by a specialist who has provided care. Patients have the right to ask the doctor to amend any part of the report that the patient considers to be incorrect or misleading, and to attach their disagreement to the report, or to withdraw their consent for the release of the information.

Adult Support and Protection (Scotland) Act 2007. This Act requires health boards in Scotland to report to local authorities if they know or believe that an adult is at risk of harm (but not necessarily incapacitated) and that action needs to be taken to protect them. The Act also requires certain public bodies and office-holders to cooperate with local authorities making enquiries about adults at risk and includes powers to examine health records for related purposes. You can read detailed guidance in the *Adult Support and Protection Code of Practice*.*

* www.gov.scot/Publications/2014/05/6492.

Adults with Incapacity (Scotland) Act 2000 and ***Mental Capacity Act 2005***. These pieces of legislation provide for information to be shared with anyone who is authorised to make decisions on behalf of, or who is appointed to support and represent, a mentally incapacitated patient. This might be a welfare attorney, a court-appointed deputy or guardian or an independent mental capacity advocate. You can read detailed guidance in the *Adults with Incapacity (Scotland) Act 2000 Code of Practice*[*] and the *Mental Capacity Act Code of Practice*.[†]

Care Act 2014. This Act requires 'relevant partners' to cooperate with local authorities making enquiries about adults at risk unless an exemption set out in the Act applies. Relevant partners include NHS trusts, foundation trusts and clinical commissioning groups in the local authority's area. Certain persons or bodies are also required to provide information to safeguarding adults boards, if the information is requested for the purpose of enabling or assisting a safeguarding adults board to perform its functions. The explanatory notes to the Act make clear that individual doctors can be asked for information under this provision. You can read detailed guidance in the *Care and Support Statutory Guidance*.[‡]

Crime and Disorder Act 1998. Section 115 permits disclosure to organisations such as the police, local authorities, or probation services but does not create a legal obligation to do so. Information should only be disclosed only if the patient consents, or there is an overriding public interest, or in response to a court order.

Criminal Law Act (Northern Ireland) 1967. Section 5 places a duty on all citizens to report to the police information they may have about the commission of a relevant offence (one with a maximum sentence of five years or more). The duty does not arise where a person has a 'reasonable excuse' not to disclose the information.

Health and Social Care Act 2012. Section 259 gives the Health and Social Care Information Centre (HSCIC) the power to require providers of health and social care in England to send it confidential data in limited circumstances including when directed to do so by the Secretary of State for Health or NHS England. Patient consent is not needed, but the HSCIC will respect patient objections to the HSCIC using their data (unless there is a legal duty or an overriding public interest to do otherwise) in line with the pledges set out in the NHS Constitution.

Health and Social Care (Safety and Quality) Act 2015. This Act places a duty on providers and commissioners of health and social care in England to share information when it is considered likely to facilitate the provision of health or social care to an individual and when it is in the individual's best interests. The duty will not apply where an individual objects (or would be likely to object), or where the information is connected with the provision of care by 'an anonymous access provider' (such as a sexual health service) or where the duty cannot be reasonably complied with for other reasons. The duty does not override duties under the common law or the *Data Protection Act 1998*.

The Information Governance Alliance has published guides to the *Health and Social Care (Safety and Quality) Act 2015* on its website.[§]

* www.gov.scot/Publications/2008/03/18094148/0.

† www.gov.uk/government/publications/mental-capacity-act-code-of-practice.

‡ www.gov.uk/government/publications/care-act-2014-statutory-guidance-for-implementation.

§ http://systems.hscic.gov.uk/infogov/iga/resources/infosharing.

Mental Health Act 1983, Mental Health (Care and Treatment) (Scotland) Act 2003 and ***Mental Health Northern Ireland Order (1986)***. These pieces of legislation provide for a number of situations in which confidential information about patients can be disclosed, even if the patient does not consent. Detailed guidance can be found in the *Mental Health Act 1983: Code of Practice*;* in the *Code of Practice under the Mental Health (Care & Treatment) (Scotland) Act 2003*† and on the website of the Mental Welfare Commission for Scotland;‡ and in the *Guidelines on the use of the Mental Health (Northern Ireland) Order 1996*.§

Road Traffic Act 1988 and ***Road Traffic (Northern Ireland Order) 1981***. In certain circumstances, all citizens (including doctors) must give the police, on request, any information that may identify a driver alleged to have committed a traffic offence.

Social Services and Well-being (Wales) Act 2014.¶ This Act requires 'relevant partners' (which include local health boards and NHS trusts in Wales) to tell local authorities if they have reasonable cause to suspect that an adult is at risk of harm (but not necessarily incapacitated). The Act also requires relevant partners to cooperate with local authorities making enquiries about adults at risk, and certain persons or bodies to provide information to safeguarding adults boards, unless an exemption set out in the Act applies. Detailed guidance can be found in the *Statutory guidance in relation to part 7 (Safeguarding) of the Social Services and Well-being (Wales) Act 2014*.

Terrorism Act 2000. There is a general obligation on all citizens under the Act to tell the police information that may help to prevent an act of terrorism, or help in apprehending or prosecuting a terrorist.

Statutory restrictions on disclosure of information about patients

Gender Recognition Act 2004. Section 22 of the Act makes it an offence to disclose 'protected information' when that information is acquired in an official capacity. 'Protected information' is defined as information about a person's application for gender recognition and a person's gender history after that person has changed gender under the Act. Section 22 also sets out a series of exceptions, where disclosure is considered to be justified. These are further expanded and clarified by Statutory Instrument 2005 No. 635

Human Fertilisation and Embryology Act 1990 (as amended). Section 33A protects the confidentiality of information kept by clinics and the Human Fertilisation and Embryology Authority (HFEA). Information may be accessed or disclosed only in the specific circumstances set out in the Act. Disclosure of information which identifies the patient in other circumstances without the patient's prior consent is a criminal offence.

The National Health Service (Venereal Diseases) Regulations 1974 and the ***NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000***. These regulations provide that any information capable of identifying an individual who is examined or treated for any sexually transmitted disease including HIV shall not be disclosed, other than to a medical practitioner in connection with the treatment of the individual or for the prevention of the spread of the disease.

* www.gov.uk/government/publications/code-of-practice-mental-health-act-1983.

† www.gov.scot/Topics/Health/Services/Mental-Health/Law/Code-of-Practice.

‡ www.mwcscot.org.uk/the-law/mental-health-act.

§ www.gain-ni.org/flowcharts/index.html.

¶ Comes into force April 2016.

Endnotes

1 Caldicott or data guardians are senior people in the NHS, local authority social care services, and partner organisations, who are responsible for protecting the confidentiality of patient information and enabling appropriate information sharing.

2 In 2013, the Caldicott principles were updated to include a new principle: *'the duty to share information can be as important as the duty to protect patient confidentiality.'*

3 Doctors working in a managed environment will do this largely by understanding and following corporate information governance and confidentiality policies.

4 The *Health and Social Care (Safety and Quality) Act 2015* created a duty to share information for direct care in England except in certain circumstances. See the legal annex to this guidance for more information.

5 All staff members receiving personal information to provide or support care are bound by a legal duty of confidence, whether or not they have contractual or professional obligations to protect confidentiality.

6 See *Good medical practice* (2013), paragraph 22. Formerly known as National Confidential Inquiries, Clinical Outcome Review Programmes are systematic reviews that are carried out with the aim of supporting changes that can help improve the quality and safety of healthcare delivery. You can find more information on the website of the Healthcare Quality Improvement Partnership.

7 Patients are entitled to access their medical records under the *Data Protection Act 1998*. See endnote 33 below.

8 The requirements of the relevant Acts – the *Adult Support and Protection (Scotland) Act 2007*, the *Social Services and Well-being (Wales) Act 2014* and the *Care Act 2014* – are summarised in the legal annex to this guidance.

9 See the *Adults with Incapacity (Scotland) Act 2000* and the *Mental Capacity Act 2005* and their respective codes of practice. There is currently no specific mental capacity legislation for Northern Ireland, where the common law duty to act in the best interests of an incapacitated patient continues. Independent mental health advocates should also be given the information listed in section 130B of the *Mental Health Act 1983*. Guidance on the roles of independent mental health advocates is given in the *Mental Health Act 1983 Code of Practice 2015*.

10 The Department of Health in England has published a consensus statement on information sharing when a patient may be at risk of suicide.

11 See *Keenan v. The United Kingdom* (2001) ECHR 242 which found that failure to provide a prisoner with adequate psychiatric care which may have prevented his suicide amounted to a breach of Article 3 of the *European Convention on Human Rights*.

12 You can read the Information Commissioner's *Anonymisation: managing data protection risk code of practice* on the website of the Information Commissioner's Office.

13 See endnote 12 above for a reference to the code of practice.

14 Delegation involves asking a colleague to anonymise or de-identify the information or seek a patient's consent. Although you will not be accountable for the actions of those you delegate to, you will still be accountable for your decision to delegate. You must be satisfied that the person you delegate to is trained and understands their responsibilities and the consequences of breaching confidentiality. See our guidance *Delegation and referral*, available at www.gmc-uk.org/guidance/ethical_guidance/21187.asp.

15 See endnote 30 below for reference to guidance on security standards.

16 The NHS Constitution in England and NHS Scotland's *The Charter of Patient Rights* and Responsibilities both set out the rights of a patient to object to how their information is used. Under the *Data Protection Act 1998,* a data subject has a right to object to processing if it causes unwarranted and substantial damage or distress. For more information see the *Guide to Data Protection* on the website of the Information Commissioner's Office for more information.

17 The Regulations that enable this power are called the *Health Service (Control of Patient Information) Regulations 2002*. Any references to 'section 251 support or the approval' actually refer to approval given under the authority of the Regulations.

18 Disclosures covered by a regulation are not in breach of the common law duty of confidentiality.

19 In Northern Ireland, the Privacy Advisory Committee advises health and social care bodies about the use of information relating to patients and clients. In the event of a complaint or challenge its advice on best practice may play an important part in assessing the propriety of a disclosure. You can read more information on the website of the Privacy Advisory Committee. In Scotland, the Public Benefit and Privacy Panel for Health and Social Care scrutinises applications for access to NHS Scotland originated data for a variety of purposes other than direct care. You can read more information on the website of the Public Benefit and Privacy Panel for Health and Social Care. Applications to individual NHS Scotland health boards for access to their data should be made through the Caldicott approval processes of the individual boards.

20 You might seek research ethics committees' advice on the ethics of disclosing and using identifiable information for research purposes. However, they cannot authorise disclosure without consent or determine if disclosure is justified in the public interest.

21 See our explanatory guidance on *Confidentiality: Disclosing records for financial and administrative purposes* and *Confidentiality: Disclosing information for employment, insurance and similar purposes*. Disclosure necessary to respond to matters raised on a patient's behalf by a Member of Parliament may be made without seeking the patient's explicit consent but you should still check with the patient if you think they would not reasonably expect the information to be disclosed. See the Information Commissioner's technical guidance note, *The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002* (pdf).

22 If any of the exceptions set out in paragraph 112 of this guidance apply you should still disclose as much of the report as you can. The Department for Work and Pensions publishes advice about reports for benefits purposes.

23 In some circumstances, patients are entitled to see a report that has been written about them under the provisions of the *Access to Medical Reports Act 1988*. See the legal annex to this guidance for more detail.

24 The Law Society of Scotland provides some guidance for solicitors on precognition in criminal cases.

25 There is no agreed definition of serious crime. *Confidentiality: NHS Code of Practice* (Department of Health, 2003) gives some examples of serious crime (including murder, manslaughter, rape and child abuse; serious harm to the security of the state and public order and 'crimes that involve substantial financial gain or loss' are mentioned in the same category). It also gives examples of crimes that are not usually serious enough to warrant disclosure without consent (including theft, fraud, and damage to property where loss or damage is less substantial).

26 You should consider the assessment of risk posed by patients made by other professionals and by groups established for that purpose, but you must make your own assessment and decision as to whether disclosure is justified. Your assessment of risk is a matter of professional judgement in which an offender's past behaviour will be a factor. The Royal College of Psychiatrists publishes guidance for psychiatrists about sharing information in the context of public protection, including participation in multi-agency public protection arrangements (MAPPA) and panels.

27 For more information, see *Consent and confidentiality in clinical genetic practice: Guidance on genetic testing and sharing genetic information – A report of the Joint Committee on Medical Genetics* (Royal College of Physicians, second edition, 2011) (pdf).

28 The Act defines a data controller as a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

29 The *Guide to data protection* is available on the website of the Information Commissioner's Office.

30 You should follow the technical guidance of the Information Commissioner's Office. The ISO 27001 Security Management Standard and the *Code of Practice for Information Security Management in ISO 27002* give detailed guidance. The Health and Social Care Information Centre in England publishes good practice guidelines on technology-specific areas of information security and information governance. It also publishes the Information Governance Toolkit for NHS organisations, which is an online system that allows NHS organisations and partners to assess themselves against Department of Health Information Governance policies and standards. In Scotland, guidance and information governance standards are collected on the Knowledge Network. In Wales, organisations are expected to use the online Caldicott-Principles Into Practice (C-PIP) assessment to measure their compliance with components of information security. GPs are required to assess their compliance with the Information Security Management System (ISMS) framework on an annual basis using the Online ISMS Toolkit.

31 *Records Management: NHS Code of Practice* (Department of Health, 2006), *Records Management: NHS Code of Practice (Scotland)* (Scottish Government, 2008), Welsh Health Circular (2000) 71: *For The Record* (National Assembly for Wales) and *Good Management, Good Records* (Department of Health, Social Services and Public Safety, 2005) all include schedules of minimum retention periods for different types of records. You should also consider any legal requirement of specialty-specific guidance that affects the period for which you should keep records. You should not keep records for longer than necessary.

32 You can find guidance on the retention and destruction of such records in *Information Management Policy – Retention and Destruction* (Department of Health, July 2015).

33 Section 7 of the *Data Protection Act 1998* gives patients the right to have access to their personal information but there are some exceptions. For example, an exemption applies if providing subject access to information about an individual's physical or mental health or condition would be likely to cause serious harm to them or to another person's physical or mental health or condition. You also do not have to supply a patient with information about another person or that identifies another person as the source of the information, unless that other person consents or it is reasonable in the circumstances to supply the information without their consent. See the Information Commissioner's technical guidance, *Dealing with subject access requests involving other people's information* (pdf).

34 The Scottish Government and NHS Scotland have published *Using email in Scotland: a good practice guide* (2014). The Professional Standards Record Body and the Health and Social Care Information Centre have published *Faster, better, safer communications, Using e-mail in health and social care* (in England) (2015). www.ehealth.scot.nhs.uk/resources/information-governance/publications/ http://theprsb.org/standards-matters/

35 There is an obvious ethical obligation. There may also be a legal obligation: see *Lewis v. Secretary of State for Health* [2008] EWHC 2196. Section 38 of the *Freedom of Information (Scotland) Act 2002* includes a deceased person's medical records within the definition of personal information, which is exempt from the general entitlement to information.

36 See paragraph 73 of *Good medical practice* (2013) and paragraph 22 of our explanatory guidance *Acting as a witness in legal proceedings* (2013).

37 The obligations associated with the statutory duty of candour in England are contained in regulation 20 of the *Health and Social Care Act 2008 (Regulated Activities) Regulations 2014*.

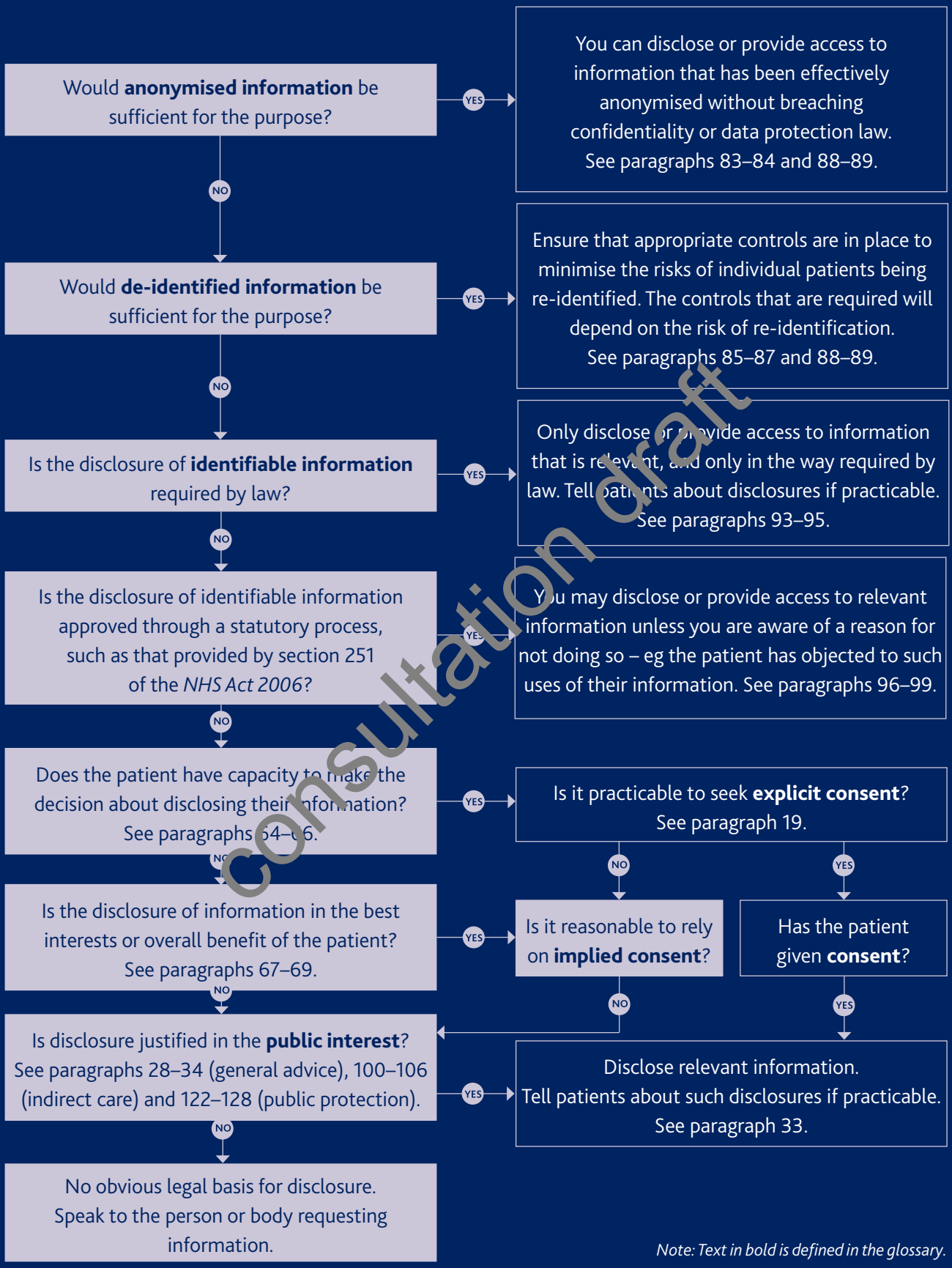
38 The permission of a surviving relative or next of kin is not required for, and does not authorise, disclosure of confidential information, although the views of those who were close to the patient may help you decide if disclosure is appropriate.

39 See our guidance *Openness and honesty when things go wrong: the professional duty of candour*.

40 See endnote 6 above for a description of Clinical Outcome Review Programmes.

41 You should contact your organisation's approved place of deposit or The National Archives, the Public Record Office of Northern Ireland or the National Archives for Scotland for further advice about storage of, and access to, archives of records of ongoing research or historical value. Health records of deceased patients are exempt from the *Freedom of Information (Scotland) Act 2002*.

What to consider before disclosing patients' personal information?



Note: Text in bold is defined in the glossary.

Email: **gmc@gmc-uk.org**
Website: **www.gmc-uk.org**
Telephone: **0161 923 6602**

Standards and Ethics Section, General Medical Council, 350 Euston Road, London NW1 3JN.

Textphone: **please dial the prefix 18001** then **0161 923 6602** to use the Text Relay service

Join the conversation

@gmcuk
facebook.com/gmcuk
linkd.in/gmcuk
youtube.com/gmcuktv

To ask for this publication in Welsh, or in another format or language, please call us on **0161 923 6602** or email us at **publications@gmc-uk.org**.

Published November 2015

GMC/CC15/1115

General Medical Council