Confidentiality:

good practice in handling patient information

General Medical Council

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.

Confidentiality: good practice in handling patient information

Published January 2017.

Came into effect 25 April 2017.

This guidance was updated on 12 October 2017. We updated paragraphs 67 and 68 to refer to *the patient's and the public interest in maintaining confidentiality*, rather than *patients' and the public interest in maintaining confidentiality*.

This guidance was updated on 25 May 2018 to reflect the requirements of the *General Data Protection Regulation and Data Protection Act 2018*.

You can find the latest version of this guidance on our website at **www.gmc-uk.org/guidance**.

Contents

About this guidance

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.

This guidance outlines the framework for considering when to disclose patients' personal information and then applies that framework to:

- **a** disclosures to support the direct care of an individual patient
- **b** disclosures for the protection of patients and others
- **c** disclosures for all other purposes.

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

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

- **a** 'You must' is used for an overriding duty or principle.
- **b** 'You should' is used when we are providing an explanation of how you will meet the overriding duty.
- **c** '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.

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, a data protection officer, your defence body or professional association, or seek independent legal advice.

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

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:

- **a** patients' fitness to drive and reporting concerns to the DVLA or DVA
- **b** disclosing information about serious communicable diseases
- **c** disclosing information for employment, insurance and similar purposes
- **d** disclosing information for education and training purposes
- **e** reporting gunshot and knife wounds
- **f** responding to criticism in the media.

Ethical and legal duties of confidentiality

1 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 their personal information will be disclosed[2] by doctors without consent, or without the chance to have some control over the timing or amount of information shared.

2 Doctors are 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.

3 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 purposes such as medical research, service planning 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.

4 Doctors' roles are continuing to evolve and change. It is likely to be more challenging to make sure there is a legal and ethical basis for using patient information in a complex health and social care environment 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.

Acting within the law

5 Doctors, like everyone else, must comply with the law when using, accessing or disclosing personal information. The law governing the use and disclosure of personal information is complex, however, and varies across the four countries of the UK.

6 In the legal annex to this guidance, we summarise some key elements of the relevant law, including the requirements of the common law, data protection law and human rights law. In the main body of the guidance, we give advice on how to apply ethical and legal principles in practice, but we do not refer to specific pieces of law unless it is necessary to do so.

7 If you are not sure how the law applies in a particular situation, you should consult a Caldicott or data guardian, a data protection officer, your defence body or professional association, or seek independent legal advice.

The main principles of this guidance

8 The advice in this guidance is underpinned by the following eight principles.[3]

- **a** **Use the minimum necessary personal information.** Use anonymised information if it is practicable to do so and if it will serve the purpose.
- **b** **Manage and protect information.** Make sure any personal information you hold or control is effectively protected at all times against improper access, disclosure or loss.
- **c** **Be aware of your responsibilities.** Develop and maintain an understanding of information governance that is appropriate to your role.
- **d** **Comply with the law.** Be satisfied that you are handling personal information lawfully.
- **e** **Share relevant information for direct care** in line with the principles in this guidance unless the patient has objected.
- **f** **Ask for explicit consent** to disclose identifiable information about patients 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.
- **g** **Tell patients** about disclosures of personal information you make that they would not reasonably expect, or check they have received information about such disclosures, unless that is not practicable or would undermine the purpose of the disclosure. Keep a record of your decisions to disclose, or not to disclose, information.
- **h** **Support patients to access their information.** Respect, and help patients exercise, their legal rights to be informed about how their information will be used and to have access to, or copies of, their health records.

Disclosing patients' personal information: a framework

When you can disclose personal information

9 Confidentiality is an important ethical and legal duty but it is not absolute. You may disclose personal information without breaching duties of confidentiality when any of the following circumstances applies.

- **a** The patient consents, whether implicitly or explicitly, for the sake of their own care or for local clinical audit (see paragraphs 13–15).
- **b** The patient has given their explicit consent to disclosure for other purposes (see paragraphs 13–15).
- **c** The disclosure is of overall benefit[4] to a patient who lacks the capacity to consent (see paragraphs 41–49).
- **d** The disclosure is required by law (see paragraphs 17–19), or the disclosure is permitted or has been approved under a statutory process that sets aside the common law duty of confidentiality (see paragraphs 20–21).
- **e** The disclosure can be justified in the public interest (see paragraphs 22–23).

10 When disclosing information about a patient you must:

- **a** use anonymised information if it is practicable to do so and if it will serve the purpose
- **b** be satisfied the patient:
  - **i** has ready access to information explaining how their personal information will be used for their own care or local clinical audit, and that they have the right to object
  - **ii** has not objected

c get the patient's explicit consent if identifiable information is to be disclosed for purposes other than their own care or local clinical audit, unless the disclosure is required by law or can be justified in the public interest
d keep disclosures to the minimum necessary for the purpose
e follow all relevant legal requirements, including the common law and data protection law.[5]

11 When you are satisfied that information should be disclosed, you should act promptly to disclose all relevant information. You should keep a record of your decision and actions.

12 You should tell patients about disclosures you make that they would not reasonably expect, or check they have received information about such disclosures, unless that is not practicable or would undermine the purpose of the disclosure – for example, by prejudicing the prevention, detection or prosecution of serious crime.

Disclosing information with a patient's consent

13 Asking for a patient's consent to disclose information shows respect, and is part of good communication between doctors and patients. Under the common law duty of confidentiality, consent may be explicit or implied.[6]

a Explicit (also known as express) consent is given when a patient actively agrees, either orally or in writing, to the use or disclosure of information.
b 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.

14 You may disclose information on the basis of implied consent for direct care when the conditions in paragraphs 28 and 29 are met, and for local clinical audit when the conditions in paragraph 96 are met. In other cases, you should ask for explicit consent to disclose personal information unless it is not appropriate or practicable to do so. For example, this might be because:

- **a** the disclosure is required by law (see paragraphs 17–19)
- **b** you are satisfied that informed consent has already been obtained by a suitable person[7]
- **c** the patient does not have capacity to make the decision. In such a case, you should follow the guidance on disclosures about patients who lack capacity to consent (see paragraphs 41–49)
- **d** you have reason to believe that seeking consent would put you or others at risk of serious harm
- **e** seeking consent would be likely to undermine the purpose of the disclosure, for example by prejudicing the prevention, detection or prosecution of a serious crime
- **f** action must be taken quickly, for example in the detection or control of outbreaks of some communicable diseases where there is insufficient time to contact the patient
- **g** seeking consent is not feasible given the number or age of records, or the likely traceability of patients
- **h** you have already decided to disclose information in the public interest (see paragraphs 63–70).

15 If you disclose personal information without consent, you must be satisfied that there is a legal basis for breaching confidentiality (see paragraph 9). You must also be satisfied that the other relevant requirements for disclosing information are met (see paragraph 10).

Disclosing information when a patient lacks the capacity to consent

16 You may disclose relevant personal information about a patient who lacks the capacity to consent if it is of overall benefit to the patient. You can find more guidance on this in paragraphs 41–49.

Disclosures required or permitted by law

17 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 87–94).

18 You should satisfy yourself that the disclosure is required by law and you should only disclose information that is relevant to the request. Wherever practicable, you should tell patients about such disclosures, unless that would undermine the purpose, for example by prejudicing the prevention, detection or prosecution of serious crime.

19 Laws and regulations sometimes permit, but do not require, the disclosure of personal information.[8] If a disclosure is permitted but not required by law, you must be satisfied that there is a legal basis for breaching confidentiality (see paragraph 9). You must also be satisfied that the other relevant requirements for disclosing information are met (see paragraph 10).

Disclosures approved under a legal process

20 You may disclose personal information without consent if the disclosure is permitted or has been approved under section 251 of the *National Health Service Act 2006* (which applies in England and Wales) or the *Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016*. These pieces of law allow the common law duty of confidentiality to be set aside for defined purposes where it is not possible to use anonymised information and where seeking consent is not practicable. There is no comparable legal framework in Scotland.

21 If you know that a patient has objected to information being disclosed for purposes other than their own care, you should not usually disclose the information unless it is required under the regulations. You can find more guidance on disclosures with specific statutory support in paragraphs 103–105.

Disclosures in the public interest

22 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 if the benefits to an individual or society outweigh both the public and the patient's interest in keeping the information confidential. For example, disclosure may be justified to protect individuals or society from risks of serious harm, such as from serious communicable diseases or serious crime. You can find guidance on disclosing information in the public interest to prevent death or serious harm in paragraphs 63–70.

23 There may also be circumstances in which disclosing personal information without consent is justified in the public interest for important public benefits, other than to prevent death or serious harm, if there is no reasonably practicable alternative to using personal information. The circumstances in which the public interest would justify such disclosures are uncertain, however, so you should seek the advice of a Caldicott or data guardian or a legal adviser who is not directly connected with the use for which the disclosure is being considered before making the disclosure. You can find further guidance in paragraphs 106–112.

Disclosures prohibited by law

24 Health professionals are required by certain laws to restrict the disclosure of some types of information. You can find examples of disclosures prohibited by law in the legal annex.

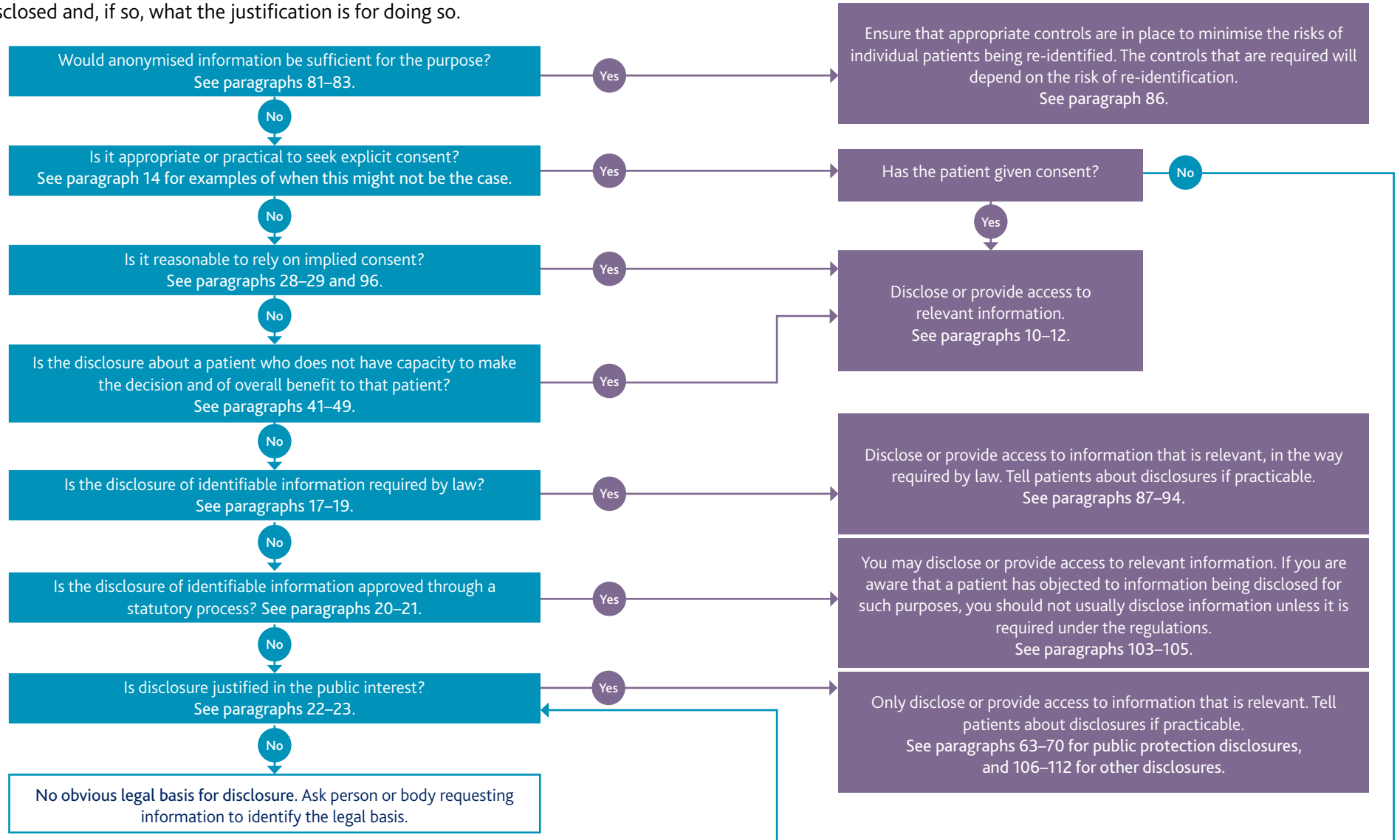
Data protection law

25 This guidance focuses on doctors' ethical and legal duties of confidentiality. But the processing of personal data must also satisfy the requirements of data protection law, which imposes various duties on data controllers. Individual doctors can be data controllers in their own right (for instance if they are partners in general practice, or hold data about patients whom they treat privately), but in many cases the data controller will be the doctor's employer. This guidance aims to be consistent with data protection law, but it is not guidance on the law. You can however find an overview of data protection law and its relationship with the common law duty of confidence in the legal annex.

Confidentiality: good practice in handling patient information

Flowchart

This flowchart can help you decide whether personal information needs to be disclosed and, if so, what the justification is for doing so.



Using and disclosing patient information for direct care

Sharing information for direct care

26 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.[9] 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.

Implied consent and sharing information for direct care

27 Most patients understand and expect that relevant information must be shared within the direct care team to provide their care.[10] You should share relevant information with those who provide or support direct care to a patient, unless the patient has objected (see paragraphs 30 and 31).[11]

28 The usual basis for sharing information for a patient's own care is the patient's consent, whether that is explicit or implied (see paragraph 13 for definitions). You may rely on implied consent to access relevant information about the patient or to share it with those who provide (or support the provision of) direct care to the patient if all of the following are met.

- **a** You are accessing the information to provide or support the individual patient's direct care, or are satisfied that the person you are sharing the information with is accessing or receiving it for this purpose.

b Information is readily available to patients, explaining how their information will be used and that they have the right to object. This can be provided in leaflets and posters, on websites, and face to face. It should be tailored to patients' identified communication requirements as far as practicable.
c You have no reason to believe the patient has objected.
d You are satisfied that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect.

29 If you suspect a patient would be surprised to learn about how you are accessing or disclosing their personal information, you should ask for explicit consent unless it is not practicable to do so (see paragraph 14). For example, a patient may not expect you to have access to information from another healthcare provider or agency on a shared record.

Patient objections to sharing information for their own care

30 If a patient objects to particular personal information being shared for their own care, you should not disclose the information unless it would be justified in the public interest,[12] or is of overall benefit to a patient who lacks the capacity to make the decision. You can find further guidance on disclosures of information about adults who lack capacity to consent in paragraphs 41–49.

31 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.

If a patient cannot be informed

32 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.

33 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.

Sharing information with those close to the patient

34 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

35 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. Early discussions about the patient's wishes can help to avoid disclosures they might object to.

Such discussions can also help avoid misunderstandings with, or causing offence or distress to, anyone the patient would want information to be shared with.

36 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.

Abiding by the patient's wishes

37 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, abide by the patient's wishes, unless disclosure would be justified in the public interest (see paragraphs 63–70).

38 If a patient lacks capacity to make the decision, it is reasonable to assume 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 to consent in paragraphs 41–49.

Listening to those close to the patient

39 In most cases, discussions with those close to the patient will take place with the patient's knowledge and consent. But if someone close to the patient wants to discuss their concerns about the patient's health without involving the patient, you should not refuse to listen to their views or concerns on the grounds of confidentiality. The information they give you might be helpful in your care of the patient.

40 You should, however, 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 should also make clear that, while it is not a breach of confidentiality to listen to their concerns, you might need to tell the patient about information you have received from others – for example, if it has influenced your assessment and treatment of the patient.[13] You should also take care not to disclose personal information unintentionally – for example, by confirming or denying the person's perceptions about the patient's health.

Disclosures about patients who lack capacity to consent

41 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 a patient lacks capacity to make a decision solely because of their age, disability, appearance, behaviour, medical condition (including mental illness), beliefs, apparent inability to communicate, or because they make a decision you disagree with.

42 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.

43 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.[14]

Considering the disclosure

44 You may disclose personal information if it is of overall benefit to a patient who lacks the capacity to consent. When making the decision about whether to disclose information about a patient who lacks capacity to consent, you must:

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

45 You must also consider:

- **a** 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
- **b** any evidence of the patient's previously expressed preferences
- **c** 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

d 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 of overall benefit to the patient

e what you and the rest of the healthcare team know about the patient's wishes, feelings, beliefs and values.

46 You might need to share personal information with a patient's relatives, friends or carers to enable you to assess the overall benefit to the patient. 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.

47 You must share relevant information with anyone who is authorised to make health and welfare decisions on behalf of, or who is appointed to support and represent, a patient who lacks capacity to give consent. This might be a welfare attorney, a court-appointed deputy or guardian, or an independent mental capacity advocate. You should also share information with independent mental health advocates in some circumstances.[15]

If a patient who lacks capacity asks you not to disclose

48 If a patient asks you not to disclose personal information about their condition or treatment, and you believe they lack capacity to make that decision, you should try to persuade them to allow an appropriate person to be given relevant information about 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 paragraph 47).

49 If the patient still does not want you to disclose information, but you consider that it would be of overall benefit to the patient and you believe they lack capacity to make that decision, 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.

Disclosures for the protection of patients and others

Disclosing information to protect patients

50 All patients have the right to a confidential medical service. Challenging situations can however 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

51 For specific guidance on confidentiality in the context of child protection, see our guidance *Protecting children and young people: the responsibilities of all doctors*.[16] 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*.[17]

Disclosing information about adults who may be at risk of harm

52 As a rule, you should make decisions about how best to support and protect adult patients in partnership with them, 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.

Legal requirements to disclose information about adults at risk

53 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.[18] You must disclose information if it is required by law.

You should:

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

54 You can find advice about disclosures that are permitted but not required by law in paragraphs 17–19.

Disclosing information to protect adults who lack capacity

55 You must disclose personal information about an adult who may be at risk of serious harm if it is required by law (see paragraph 53). Even if there is no legal requirement to do so, you must give information promptly to an appropriate responsible person or authority if you believe a patient who lacks capacity to consent is experiencing, or at risk of, neglect or physical, sexual or emotional abuse, or any other kind of serious harm, unless it is not of overall benefit to the patient to do so.

56 If you believe it is not of overall benefit to 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.

The rights of adults with capacity to make their own decisions

57 As a principle, adults who have capacity are entitled to make decisions in their own 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 in paragraph 14.

58 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.

59 You should, however, usually abide by 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.[19, 20] 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.[21] Adults who initially refuse offers of assistance may change their decision over time.

Disclosing information to protect others

60 Doctors owe a duty of confidentiality to their patients, but they also have a wider duty to protect and promote the health of patients and the public.[22]

Legal requirements to disclose information for public protection purposes

61 Some laws require disclosure of patient information for purposes such as the notification of infectious diseases and the prevention of terrorism. You must disclose information if it is required by law, including by the courts (see paragraphs 87–94).

Disclosing information with consent

62 You should ask for a patient's consent to disclose information for the protection of others unless the information is required by law or it is not safe, appropriate or practicable to do so (see paragraph 14). You should consider any reasons given for refusal.

Disclosing information in the public interest

63 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.[23]

64 If it is not practicable or appropriate to seek consent, and in exceptional cases where a patient has refused consent, disclosing personal information may be justified in the public interest if failure to do so may expose others to a risk of death or serious harm. The benefits to an individual or to society of the disclosure must outweigh both the patient's and the public interest in keeping the information confidential.

65 Such a situation might arise, for example, if a disclosure would be likely to be necessary for the prevention, detection or prosecution of serious

crime, 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.

66 Other examples of situations in which failure to disclose information may expose others to a risk of death or serious harm include when a patient is not fit to drive,[24] or has been diagnosed with a serious communicable disease,[25] or poses a serious risk to others through being unfit for work.[26]

67 Before deciding whether disclosure would be justified in the public interest you should consider whether it is practicable or appropriate to seek consent (see paragraph 14). You should not ask for consent if you have already decided to disclose information in the public interest but you should tell the patient about your intention to disclose personal information, unless it is not safe or practicable to do so. If the patient objects to the disclosure you should consider any reasons they give for objecting.

68 When deciding whether the public interest in disclosing information outweighs the patient's and the public interest in keeping the information confidential, you must consider:

- **a** 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
- **b** 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
- **c** the potential harm to others (whether to a specific person or people, or to the public more broadly) if the information is not disclosed

- **d** the potential benefits to an individual or to society arising from the release of the information
- **e** the nature of the information to be disclosed, and any views expressed by the patient
- **f** whether the harms can be avoided or benefits gained without breaching the patient's privacy or, if not, what is the minimum intrusion.

If you consider that failure to disclose the information would leave individuals or society exposed to a risk so serious that it outweighs the patient's and the public interest in maintaining confidentiality, you should disclose relevant information promptly to an appropriate person or authority.

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

70 Decisions about whether or not disclosure without consent can be justified in the public interest can be complex. 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 the patient.

Responding to requests for information

71 You must consider seriously all 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).[27] You must also consider seriously all requests for information needed for formal reviews (such as inquests and inquiries, serious or significant case reviews, case management reviews, and domestic homicide reviews) that are established to learn lessons and to improve systems and services.

72 If you disclose personal information without consent, you must be satisfied that there is a legal basis for breaching confidentiality (see paragraph 9). You must also be satisfied that the other relevant requirements for disclosing information are met (see paragraph 10).

Disclosing genetic and other shared information

73 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.

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

- **a** get prophylaxis or other preventative treatments or interventions
- **b** make use of increased surveillance or other investigations
- **c** prepare for potential health problems.[28]

75 If a patient refuses to consent to information being disclosed that would benefit others, disclosure might still be justified in the public interest if failure to disclose the information leaves others at risk of death or serious harm (see paragraphs 63–70). 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.

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

Using and disclosing patient information for secondary purposes

77 Many important uses of patient information contribute to the overall delivery of health and social care. Examples include health services management, research, epidemiology, public health surveillance, and education and training. Without information about patients the health and social care system would be unable to plan, develop, innovate, conduct research or be publicly accountable for the services it provides.

78 There are also important 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 the administration of justice, and for purposes such as financial audit and insurance or benefits claims.

79 Anonymised information will usually be sufficient for purposes other than the direct care of the patient and you must use it in preference to identifiable information wherever possible. If you disclose identifiable information, you must be satisfied that there is a legal basis for breaching confidentiality.

80 You may disclose personal information without breaching duties of confidentiality when any of the following circumstances apply.

- **a** The disclosure is required by law, including by the courts (see paragraphs 87–94).
- **b** The patient has given explicit consent (see paragraph 95).
- **c** The disclosure is approved through a statutory process that sets aside the common law duty of confidentiality (see paragraphs 103–105).
- **d** The disclosure can, exceptionally, be justified in the public interest (see paragraphs 106–112).

You must also be satisfied that the other relevant requirements for disclosing information are met (see paragraph 10).

Anonymised information

81 The Information Commissioner's Office anonymisation code of practice (ICO code) considers data to be anonymised if it does not itself identify any individual, and if it is unlikely to allow any individual to be identified through its combination with other data.[29] Simply removing the patient's name, age, address or other personal identifiers is unlikely to be enough to anonymise information to this standard.[30]

82 The ICO code also makes clear that different types of anonymised data pose different levels of re-identification risk. For example, data sets with small numbers may present a higher risk of re-identification than large data sets. The risk of re-identification will also vary according to the environment in which the information is held. For example, an anonymised data set disclosed into a secure and controlled environment could remain anonymous even though the same data set could not be made publically available because of the likelihood of individuals being identified.

83 You should follow the ICO code, or guidance that is consistent with the ICO code, or seek expert advice, if you have a role in anonymising information or disclosing anonymised information.

The process of anonymising information

84 Information may be anonymised by a member of the direct care team who has the knowledge, skills and experience to carry out the anonymisation competently, or will be adequately supervised.

85 If it is not practicable for the information to be anonymised within the direct care team, it may be anonymised by a data processor under contract, as long as there is a legal basis for any breach of confidentiality (see paragraph 80), the requirements of data protection law are met (see the legal annex) and appropriate controls are in place to protect the information (see paragraph 86).

Disclosing anonymised information

86 If you decide to disclose anonymised information, you must be satisfied that appropriate controls are in place to minimise the risk of individual patients being identified. The controls that are needed will depend on the risk of re-identification, and might include signed contracts or agreements that contain controls on how the information will be used, kept and destroyed, as well as restrictions to prevent individuals being identified. You should refer to specialist advice or guidance when assessing risk, or considering what level of control is appropriate.[31]

Disclosures required by statutes or the courts

Disclosure required by statute

87 There are a large number of laws that require disclosure of patient information – for purposes as diverse as the notification of infectious diseases, the provision of health and social care services, the prevention of terrorism and the investigation of road accidents.

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

- **a** satisfy yourself that personal information is needed, and the disclosure is required by law
- **b** only disclose information relevant to the request, and only in the way required by the law

c tell patients about such disclosures whenever practicable, unless it would undermine the purpose of the disclosure to do so
d abide by patient objections where there is provision to do so.[32]

89 You can find advice about disclosures that are permitted but not required by law in paragraph 19.

Disclosing information to the courts, or to obtain legal advice

90 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.

91 You should only disclose information that is required by the 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 disclosing the information might put someone at risk of harm.

92 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 what information you will disclose in response to the order, unless that is not practicable or would undermine the purpose for which disclosure is sought.

93 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 ordered by a court, or can be justified in the public interest. You may disclose information without consent to your own legal adviser to get their advice.

94 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, but 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 may disclose.[33]

Consent

95 You should ask for consent to disclose personal information for purposes other than direct care[34] or local clinical audit unless the information is required by law, or it is not appropriate or practicable to obtain consent (see paragraph 14 for examples of when this might be the case).

Disclosures for health and social care secondary purposes

Clinical audit

96 All doctors in clinical practice have a duty to participate in clinical audit[35] and to contribute to clinical outcome review programmes.[36] If an audit is to 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 on the basis of implied consent, as long as you are satisfied that it is not practicable to use anonymised information and that the patient:

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

97 If a patient does object to personal information about them being included in a local clinical audit related to their care, you should explain why the information is needed and how this may benefit their current and future care. If the patient still objects, you should remove them from the audit if practicable. If that is not practicable, you should make sure this is explained to the patient, along with any options open to them.

98 If a clinical audit is to be carried out, but not by the team that provided care or those working to support them, the information should be anonymised. If this is not practicable, or if personal information is essential to the audit, you should disclose the information only if you have the patient's explicit consent or if there is another legal basis for breaching confidentiality (see paragraph 80). You must also be satisfied that the other relevant requirements for disclosing information are met (see paragraph 10).

Disclosures for financial or administrative purposes

99 If you are asked to disclose information about patients for financial or administrative purposes, you should give it in an anonymised form, if that is practicable and will serve the purpose. If identifiable information is needed, you must be satisfied that there is a legal basis for breaching confidentiality (see paragraph 80).[37] You must also be satisfied that the other relevant requirements for disclosing information are met (see paragraph 10).

The professional duty of candour and confidentiality

100 All doctors have a duty of candour – a professional responsibility to be honest with patients when things go wrong. As part of this duty, doctors must tell the patient when something has gone wrong, and explain the short- and long-term effects of what has happened.[38]

101 If the patient has died, or is unlikely to regain consciousness or capacity, it may be appropriate to speak to those close to the patient. When providing information for these purposes, you should still respect the patient's confidentiality. If a patient has previously asked you not to share personal information about their condition or treatment with those close to them, you should abide by their wishes. You must still do your best to be considerate, sensitive and responsive to those close to the patient, giving them as much information as you can.

Openness and learning from adverse incidents and near misses

102 A number of reporting systems and schemes exist around the UK for reporting adverse incidents and near misses. Organisations also have policies for reporting and responding to adverse incidents and near misses and in some cases organisational duties of candour have been written into law.[39] If the law requires personal information to be disclosed for these purposes, you should follow the guidance in paragraph 87. If the law does not require it, you should ask for consent to disclose personal information unless it is not appropriate or practicable to do so (see paragraph 14). In exceptional cases, disclosure may be justified without consent in the public interest (see paragraphs 106–112).

Disclosures with specific statutory support

103 In England, Wales and Northern Ireland, statutory arrangements are in place for considering whether disclosing personal information without consent for health and social care purposes would benefit patients or the public sufficiently to outweigh patients' right to privacy. Examples of these purposes include medical research, and the management of health or social care services. There is no comparable statutory framework in Scotland.

104 Section 251 of the *National Health Service Act 2006* (which applies in England and Wales) and the *Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016* allow the common law duty of confidentiality to be set aside for defined purposes where it is not possible to use anonymised information and where seeking consent is not practicable. You can find more detail about these statutory arrangements in the legal annex.

105 You may disclose personal information without consent if the disclosure is permitted or has been approved under regulations made under section 251 of the *National Health Service Act 2006* or under the *Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016*. If you know that a patient has objected to information being disclosed for purposes other than direct care, you should not usually disclose the information unless it is required under the regulations.[40]

Public interest disclosures for health and social care purposes

106 In exceptional circumstances, there may be an overriding public interest in disclosing personal information without consent for important health and social care purposes if there is no reasonably practicable alternative

to using personal information and it is not practicable to seek consent. The benefits to society arising from the disclosure must outweigh the patient's and public interest in keeping the information confidential.

107 You should not disclose personal information without consent in the public interest if the disclosure falls within the scope of any of the regulations described in paragraphs 103–105, and the disclosure is not permitted, or has not been approved, under those regulations.

108 If the regulations described in paragraphs 103–105 do not apply, you may need to make your own decision about whether disclosure of personal information without consent is justified. The circumstances in which the public interest would justify such disclosures are uncertain, however, so you should seek the advice of a Caldicott or data guardian or a legal adviser who is not directly connected with the use for which the disclosure is being considered before making the disclosure.[41]

109 Before considering whether disclosing personal information without consent may be justified in the public interest, you must satisfy yourself that it is either necessary to use identifiable information or not reasonably practicable to anonymise the information. In either case, you must be satisfied that it is not reasonably practicable to seek consent.[42]

110 When considering whether disclosing personal information without consent may be justified in the public interest, you must take account of the factors set out in paragraph 67. You must also be satisfied that:

- **a** the disclosure would comply with the requirements of data protection law and would not breach any other legislation that prevents the disclosure of information about patients (see the legal annex for examples)
- **b** the disclosure is the minimum necessary for the purpose

c the information will be processed in a secure and controlled environment that has the capabilities and is otherwise suitable to process the information (see paragraph 86)
d information is readily available to patients about any data that has been disclosed without consent, who it has been disclosed to, and the purpose of the disclosure.

111 If you know that a patient has objected to information being disclosed for purposes other than their own care, you should not disclose information in the public interest unless failure to do so would leave others at risk of death or serious harm (see paragraphs 63–70).

112 You must keep a record of what information you disclosed, your reasons, and any advice you sought.

Ethical approval for research

113 You should only disclose personal information for research if there is a legal basis for the disclosure and the research has been approved by a research ethics committee.

114 If you are applying for ethical approval for research, you should let the research ethics committee know if personal information will be disclosed without consent and tell them the legal basis for the disclosure.

Requests from employers, insurers and other third parties

115 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:

- **a** 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
- **b** 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
- **c** 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,[43] 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
- **d** 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:
  - **i** they have already indicated they do not wish to see it
  - **ii** disclosure would be likely to cause serious harm to the patient or anyone else
  - **iii** disclosure would be likely to reveal information about another person who does not consent.[44, 45]

116 If a patient refuses or withdraws consent, or if it is not practicable to get their consent, you may still disclose information if it can be justified in the public interest (see paragraphs 63–70). You must disclose information if it is required by law (see paragraphs 87–94).

Managing and protecting personal information

Improper access and disclosure

117 Health and care records can include a wide range of material, including but not limited to:

- **a** handwritten notes
- **b** electronic records
- **c** correspondence between health professionals
- **d** visual and audio recordings
- **e** laboratory reports
- **f** communications with patients (including texts and emails).

118 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.

119 You must make sure any personal information about patients that you hold or control is effectively protected at all times against improper access, disclosure or loss. 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.

120 You must not access a patient's personal information unless you have a legitimate reason to view it.

121 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.[46] While there are some practice environments in which it may be difficult to avoid conversations with (or about) patients being overheard by others, you should try to minimise breaches of confidentiality and privacy as far as it is possible to do so.

Knowledge of information governance and raising concerns

122 You must develop and maintain an understanding of information governance that is appropriate to your role.

123 You should be satisfied that any members of staff you manage are trained and understand their information governance responsibilities. 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 law.

124 Unless you have a role in commissioning or managing systems, 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. If, however, you are concerned about the security of personal information in premises or systems provided for your use, or the adequacy of staff training on information governance, you should follow our advice in *Raising and acting on concerns about patient safety*.[47]

Processing information in line with data protection law

125 The *General Data Protection Regulation* read with the *Data Protection Act 2018* sets out the responsibilities of data controllers[48] when processing personal data, as well as a number of rights for individuals (known as data subjects). Detailed guidance is available on the website of the Information Commissioner's Office (ICO).[49] You can find a summary of the data protection principles in the legal annex to this guidance.

126 If you are a data controller, you must understand and meet your obligations under data protection law. This includes responsibilities to make sure patients' personal information that you hold is handled in ways that are transparent and in ways that patients would reasonably expect, and appropriate technical and organisational measures are in place to guard against data loss. You must also make sure information is readily available to patients that explains how their information is processed, including:

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

When deciding how to provide this information, you should take into account the ICO's guidance on fair processing or privacy notices.[50]

127 Whether or not you are a data controller, you must 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.

Records management and retention

128 If you are responsible for managing patient records or other patient information, you must make sure the records you are responsible for are made, stored, transferred, protected and disposed of in line with data protection law and other relevant laws. You should make use of professional expertise when selecting and developing systems to record, access and send electronic data.[51]

129 You must make sure 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.[52] You should make sure administrative information, such as names and addresses, can be accessed separately from clinical information so that sensitive information is not displayed automatically.

130 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.[53]

The rights of patients to access their own records

131 Patients have a right to access their own health records, subject to certain safeguards.[54] You should respect, and help patients to exercise, their legal rights to have access to, or copies of, their health records. The ICO gives guidance on what fees you may charge.

Communicating with patients

132 Wherever possible, you should communicate with patients in a format that suits them. For example, electronic communications – such as email or text messaging – can be convenient and can support effective communication between doctors and patients, with appropriate safeguards.[55]

133 Most communication methods pose some risk of interception – for example, messages left on answering machines can be heard by others and emails can be insecure. You should take reasonable steps to make sure the communication methods you use are secure.

Disclosing information after a patient has died

134 Your duty of confidentiality continues after a patient has died.[56]

135 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[57]
- 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
- when disclosure is necessary to meet a statutory duty of candour.[58]

136 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 abide by their wishes. If you are unaware of any instructions from the patient, when you are considering requests for information you should take into account:

- **a** whether disclosing information is likely to cause distress to, or be of benefit to, the patient's partner or family[59]
- **b** whether the disclosure will also disclose information about the patient's family or anyone else
- **c** whether the information is already public knowledge or can be anonymised or de-identified
- **d** the purpose of the disclosure.

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

- the disclosure is permitted or has been approved under a statutory process that sets aside the common law duty of confidentiality, unless you know the patient has objected (see paragraphs 103–105)
- when disclosure is justified in the public interest to protect others from a risk of death or serious harm
- for public health surveillance, in which case the information should be anonymised, unless that would defeat the purpose
- when a parent asks for information about the circumstances and causes of a child's death
- when someone close to an adult patient asks for information about the circumstances of that patient's death, and you have no reason to believe the patient would have objected to such a disclosure
- when disclosure is necessary to meet a professional duty of candour (see paragraphs 100 and 101)

- when it is necessary to support the reporting or investigation of adverse incidents, or complaints, for local clinical audit, or for clinical outcome review programmes.[60]

138 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.[61]

Legal annex

There is no overarching law that governs the disclosure of confidential information. The common law and other laws 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.

We have also published a more detailed factsheet, *Confidentiality: key legislation*, which you can find on our confidentiality guidance page at **www.gmc-uk.org/guidance**.

Sources of law on confidentiality, data protection and privacy

The common law

Information acquired by doctors in their professional capacity will generally be confidential under the common law. 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. This means a doctor must not disclose confidential information, unless there is a legal basis for doing so.

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

- **a** the patient consents
- **b** it is required by law, or in response to a court order
- **c** it is justified in the public interest.

But the common law cannot be considered in isolation. Even if a disclosure of confidential information is permitted under the common law, the disclosure must still satisfy the requirements of data protection law.

Data protection law (UK)

The General Data Protection Regulation (GDPR), supplemented by the *Data Protection Act 2018*, 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 Information Commissioner's Office (ICO) is the authority responsible for upholding information rights in the UK. Detailed guidance on complying with data protection law is available on the ICO website: www.ico.org.uk.

The GDPR defines personal data as:

> 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'

The GDPR defines a data controller as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. Individual doctors can be data controllers in their own right (for example, if they are partners in general practice, or hold data in relation to patients whom they treat privately) but in many cases the data controller will be the doctor's employer.

The GDPR is based around six data protection principles and provides a range of rights for individuals. The principles state that personal data must:

- be processed lawfully, fairly and in a transparent manner
- be processed for specified, explicit and legitimate purposes and not in any manner incompatible with those purposes
- be adequate, relevant and limited to what is necessary in relation to the purposes
- be accurate and up to date
- not be kept for longer than is necessary
- be secure.

The first principle of the GDPR states that data must be processed lawfully and fairly. This means:

a patients' information must not be processed in a way that breaches either statute or common law. For example, if disclosing information would be a breach of the common law duty of confidentiality, it would also be unlawful under data protection law

b patients' personal information must be handled in ways that are transparent and in ways they would reasonably expect.

One or more of the conditions for processing in Article 6 (for all personal data) and Article 9 (for 'special category data', which includes health data) to the GDPR must also be met for the processing to be fair and lawful.

In all cases where personal data is processed, at least one of the conditions set out in Article 6 must be met. The conditions most likely to be relevant in medical practice are that:

- the data subject has given consent (Article 6(1)(a))
- the processing is necessary for the performance of a contract (Article 6(1)(b))
- the processing is necessary because of a legal obligation that applies to the data controller (except an obligation imposed by a contract) (Article 6(1)(c))
- the processing is necessary to protect the vital interests of the data subject (Article 6(1)(d))
- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6 (1)(e))
- the processing is necessary for the purposes of legitimate interests pursued by the data controller or a third party (Article 6 (1)(f)).

Where special category data are being used, at least one of the conditions in Article 9 must also be met. Information on a patient's health record is likely to be special category data for the purposes of the GDPR. The conditions most likely to be relevant in medical practice are that:

- the data subject has given explicit consent (Article 9(2)(a))
- the processing is necessary to protect the vital interests of the data subject or another person in a case where the data subject is physically or legally incapable of giving consent (Article 9(2)(c))

- the processing is necessary for reasons of substantial public interest (Article 9(2)(g))
- the processing is necessary for medical purposes where the processing is undertaken by a health professional or someone else who owes an equivalent duty of confidentiality (Article 9 (2)(h))
- the processing is necessary for reasons of public interest in the area of public health (Article 9(2)(i))
- the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 9(2)(j)).

The *Data Protection Act 2018* sets out more specific requirements which must also be met when a data controller is relying on the public interest and health conditions in Article 9. In some circumstances a data controller is required under the *Data Protection Act 2018* to produce an 'appropriate policy document' which sets out the compliance measures in place to protect the data. This requirement does not apply if the disclosure of sensitive personal data uses the health-related conditions for processing, but it does apply if an employment related condition is relied on. The interactions between the GDPR and *Data Protection Act 2018* are complex and data controllers should seek specialist advice where appropriate.

Consent under the GDPR

The standard of consent under the GDPR is higher than under the common law of confidentiality. The GDPR defines consent as:

> 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'

The GDPR also sets out a number of other conditions for consent.

- The controller must be able to demonstrate that the data subject has consented to the processing of personal data.
- Consent can be withdrawn at any time (this doesn't affect lawfulness of processing before withdrawal). Prior to giving consent, data subjects must be informed of their right to withdraw. It must be as easy to withdraw consent as to give it.
- Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

It will not always be appropriate for data controllers to rely on consent under GDPR as a condition for processing health data. For example, implied consent is an accepted concept under the law of confidentiality, but it is unlikely to be a sufficient basis for sharing personal data based on consent under Article 6(1)(a) of the GDPR, and will not be sufficient for sharing 'special category data' based on explicit consent under Article 9(2)(a) of the GDPR. However, the GDPR does provide alternative conditions for processing data which are likely to be more appropriate in a health context.

This means that a doctor who is a data controller may be relying on different legal justifications for disclosing information under the common law duty of confidence and under the GDPR. It also means that doctors can continue to share information on the basis of implied consent if the conditions set out in paragraphs 28 and 29 (for direct care) and 96 (for local clinical audit) of this guidance are met.

Other requirements imposed by the GDPR

The GDPR imposes a number of other requirements on data controllers, and confers various rights on data subjects. A full summary of the GDPR is outside the scope of this guidance, but detailed guidance is provided by the ICO: www.ico.org.uk.

Human Rights Act 1998 (UK)

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 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.

Relevant factors to take into account when considering a disclosure in the public interest are given in paragraphs 63–70, and 106–112 of this guidance.

Other ECHR rights that may be relevant to considerations about whether disclosing 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 Acts across the UK

The *Freedom of Information Act 2000 (England, Northern Ireland and Wales) and Freedom of Information (Scotland) Act 2002* give public access to information held by public authorities. Public authorities include government departments, local authorities, the NHS, state schools and police forces. The Acts do 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*. You can find guidance about the *Freedom of Information Act 2000* on the ICO website: www.ico.org.uk. Guidance about the *Freedom of Information (Scotland) Act 2002* is available on the website of the Scottish Information Commissioner at www.itspublicknowledge.info.

Computer Misuse Act 1990 (UK)

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.

Regulation of healthcare providers and professionals

Various bodies regulating healthcare providers and professionals have legal powers to require information to be disclosed, 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) in England 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. You can find the code of practice on the CQC's website: www.cqc.org.uk.

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** in Northern Ireland 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, 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 Authority** 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 the Welsh Assembly Government have published codes of practice for the use of these powers. There are no comparable specific powers to require the production of documents for these purposes in Scotland or Northern Ireland.

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 Public Services 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.

Laws on disclosure for health and social care purposes

Health and Social Care Act 2012 (England)

Section 259 gives the Health and Social Care Information Centre (known as NHS Digital) 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 UK Secretary of State for Health or NHS England. Patient consent is not needed, but patient objections will be handled in line with the pledges set out in the *NHS Constitution for England* and directions given to NHS Digital by the Secretary of State.

Health and Social Care (Safety and Quality) Act 2015 (England)

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.digital.nhs.uk/information-governance-alliance.

Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016

This Act requires the Department of Health in Northern Ireland to make regulations that permit or require the processing of confidential information for defined health and social care purposes. The Act allows the common law duty of confidentiality to be set aside where seeking individuals' consent is not practicable, where it is not possible to use anonymised information and where the committee established under the Act has authorised the processing. The Act does not set aside the *Data Protection Act 1998* or the *Human Rights Act 1998* and any use of information must continue to comply with the requirements of these two pieces of legislation.

No regulations have yet been made under the Act. Until such regulations are made the Privacy Advisory Committee will continue to advise health and social care bodies about the use of information relating to patients and clients. You can find out more about the committee on its website: www.privacyadvisorycommittee.hscni.net.

Section 251 of the *NHS Act 2006* (England and Wales)

Section 251 of this Act allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes. In practice, this means the person responsible for the information can disclose confidential patient information without consent to an applicant without being in breach of the common law duty of confidentiality, as long as the requirements of the regulations are met. The person responsible for the information must still comply with all other relevant legal obligations such as the *Data Protection Act 1998* and the *Human Rights Act 1998*.

The regulations that enable this power are called the *Health Service (Control of Patient Information) Regulations 2002*. Any references to 'section 251 support or approval' actually refer to approval given under the authority of the regulations. These powers can only be used where it is not practical to obtain consent and anonymised information cannot be used, having regard to the cost and available technology. They cannot be used to permit information to be disclosed solely or principally for the direct care of individual patients. The regulations only apply in England and Wales.

The regulations provide different kinds of support.

- Regulation 2 provides specific support for cancer registries to receive and process identifiable data on patients referred for the diagnosis or treatment of cancer for the medical purposes set out in the regulation.
- Regulation 3 provides specific support for identifiable patient information to be disclosed to, and processed by, the persons or bodies listed in paragraph 3 of Regulation 3 when processing is intended to diagnose, control or prevent, or recognise trends in, communicable diseases and other risks to public health.
- Regulation 5 can be used to permit processing for a range of medical purposes, broadly defined to include 'preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services'. Any person wishing to obtain support under Regulation 5 will submit an application to the Confidentiality Advisory Group of the Health Research Authority. The Confidentiality Advisory Group will then give advice to the relevant decision maker, which is currently the Health Research Authority for research applications and the Secretary of State for Health for non-research applications.

> The Confidentiality Advisory Group will not usually authorise disclosures under Regulation 5 to which the patient has objected. The Health Research Authority may not give an approval unless a research ethics committee has approved the medical research concerned.

You can find more information about section 251 of the *NHS Act 2006* and the role of the Confidentiality Advisory Group on the website of the Health Research Authority: www.hra.nhs.uk.

Statutory restrictions on disclosing information about patients

Gender Recognition Act 2004 (UK)

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 *The Gender Recognition (Disclosure of Information) (England, Wales and Northern Ireland) Order 2005* and *The Gender Recognition (Disclosure of Information) (Scotland) Order 2005*.

Human Fertilisation and Embryology Act 1990 (UK)

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

The ***National Health Service (Venereal Diseases) Regulations 1974*** (Wales) and the ***NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000*** (England)

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 in relation to that disease or for the prevention of the spread of the disease.

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. Data protection officers have a statutory function under the General Data Protection Regulation to monitor a data controller's compliance with the GDPR.

2. In this guidance, 'personal information' means information from which individuals can be identified either in itself or in combination with other available information. 'Disclosure' means 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.

3. These principles are aligned with the Caldicott principles for information governance within health and social care.

4. We use the term 'overall benefit' to describe the ethical basis on which decisions are made about treatment and care for adult patients who lack capacity to decide. Our guidance on overall benefit is consistent with the legal requirement to consider whether treatment 'benefits' a patient (as the term is used in the *Adults with Incapacity (Scotland) Act 2000*), or is in the patient's 'best interests' (as the term is used in the *Mental Capacity Act 2005* in England and Wales, and in the common law in Northern Ireland). The use of the term is also consistent with the legal requirement to apply the other principles set out in the *Mental Capacity Act 2005* and *Adults with Incapacity (Scotland) Act 2000.*

5. Doctors working in a managed environment will do this largely by understanding and following this guidance and corporate information governance and confidentiality policies. Doctors who are themselves data controllers are personally responsible for understanding and meeting their responsibilities under data protection law. See the legal annex to this guidance for more information.

6. Implied consent is not likely to be sufficient to share personal data under Article 6 of the GDPR and is not sufficient to share 'special category data' such as health data under Article 9 of the GDPR. However, other conditions for processing health data are likely to apply. See the legal annex for more detail.

7. See paragraph 115 of this guidance and our explanatory guidance *Delegation and referral* (2012). You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

8. An example is the *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.

9. 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.'*

10. In this guidance, 'direct care' refers to activities that directly contribute to the diagnosis, care and treatment of an individual. The direct care team is made up of those health and social care professionals who provide direct care to the patient, and others, such as administrative staff, who directly support that care.

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

12. For example, if staff providing treatment may be at risk of serious harm which cannot be managed through the use of universal precautions. See our explanatory guidance *Disclosing information about serious communicable diseases.* You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

13. Patients are also entitled to access their health records under data protection law. See endnote 54.

14. The main provisions of the *Mental Capacity Act (Northern Ireland) 2016* have not yet come into force. The common law duty to act in the best interests of a patient who lacks capacity to consent therefore continues until the Act is commenced.

15. 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.*

16. *Protecting children and young people: the responsibilities of all doctors* (General Medical Council, 2012). You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

17. *0–18 years: guidance for all doctors* (General Medical Council, 2007). You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

18. 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 *Confidentiality: key legislation* factsheet, which you can find on our GMC confidentiality guidance page at www.gmc-uk.org/guidance.

19. In very exceptional circumstances, disclosure without consent may be justified in the public interest to prevent a serious crime such as murder, manslaughter or serious assault even where no one other than the patient is at risk. This is only likely to be justifiable where there is clear evidence of an imminent risk of serious harm to the individual, and where there are no alternative (and less intrusive) methods of preventing that harm. This is an uncertain area of law and, if practicable, you should seek independent legal advice before making such a disclosure without consent.

20. The Department of Health in England has published *Information sharing and suicide prevention: consensus statement* (2014), which is consistent with the principles in this guidance.

21. Safelives has published guidance on disclosing information to multi-agency risk assessment conferences (MARACs), which are local meetings established to discuss how to help individuals who are at high risk of murder or serious harm. The guidance is available on the Safelives website, www.safelives.org.uk. Personal information may be disclosed to a MARAC with consent, or if the disclosure can be justified in the public interest (see paragraphs 63–70 in this guidance).

22. See 'The duties of a doctor registered with the General Medical Council' at the front of this guidance.

23. There is no agreed definition of 'serious crime'. *The Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures* (Department of Health, 2003) gives some examples of serious crime. These include crimes that cause serious physical or psychological harm to individuals (such as murder, manslaughter, rape and child abuse); and crimes that cause serious harm to the security of the state and public order; and 'crimes that involve substantial financial gain or loss' are also 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).

24. We give specific advice on reporting concerns about patients' fitness to drive in our explanatory guidance *Confidentiality: Patients' fitness to drive and reporting concerns to the DVLA or DVA*. That guidance deals specifically with drivers on the roads, but the

same principles apply to drivers and pilots of other kinds of regulated transport, including by rail, water and air. You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

25. See our explanatory guidance *Confidentiality: disclosing information about serious communicable diseases.* See endnote 24 for the web address.

26. See our explanatory guidance *Confidentiality: disclosing information for employment, insurance and similar purposes.* See endnote 24 for the web address.

27. 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. You can find this in *Good Psychiatric Practice: Confidentiality and Information Sharing* (Royal College of Psychiatrists, second edition, 2010).

28. 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).

29. You can find the Information Commissioner's Office (ICO) *Anonymisation: managing data protection risk code of practice* (2012) on the ICO website at www.ico.org.uk.

30. Other potential identifiers include the patient's initials, postcode, NHS or CHC number, local identifiers (such as hospital numbers), national insurance number, and key dates (such as birthdate, date of diagnosis or date of death).

31. See endnote 29 for the reference to ICO guidance.

32. The NHS Constitution for 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 data protection law, 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 ICO website at www.ico.org.uk.

33. The Law Society of Scotland gives some guidance for solicitors on precognition in criminal cases, which you can find in the rules and guidance section of its website at

www.lawscot.org.uk.

34. See endnote 10 for the definition of 'direct care' in this guidance. Guidance on sharing information for direct care purposes is given in paragraphs 26–33.

35. In this guidance 'clinical audit' means the evaluation of clinical performance against standards or through comparative analysis, to inform the management of services.

36. 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 at www.hqip.org.uk. You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

37. Commissioners have limited rights to request personal information held by general practices for defined purposes, although they should usually respect patients' objections. See the directions on confidentiality and disclosure of information and the code of practice for the relevant country for more information. *Confidentiality and Disclosure of Information (General Medical Services, Personal Medical Services, Alternative Provider Medical Services) Directions 2013* and *Code of Practice (Department of Health, 2013)*; *Confidentiality and Disclosure of Information: General Medical Services and Alternative Provider Medical Services Directions (Northern Ireland) 2006* and *Code of Practice (Department of Health, Social Services and Public Safety, 2006)*; *Confidentiality and Disclosure of Information: General Medical Services (GMS), Section 17c Agreements, and Health Board Primary Medical Services (HBPMS) Code of Practice and Directions*; *Confidentiality and Disclosure of Information: General Medical Services and Alternative Provider Medical Services Directions 2006* and *Code of Practice (Welsh Assembly Government, 2005).*

38. We give guidance on professional and organisational duties of candour in *Openness and honesty when things go wrong: the professional duty of candour* (General Medical Council and Nursing and Midwifery Council, 2015). You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

39. 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.* In Scotland they are contained in section 22 of the *Health (Tobacco, Nicotine etc. and Care) (Scotland) Act 2016.*

40. Disclosures permitted under regulations 2 and 3 of the *Health Service (Control of Patient Information) Regulations 2002* may, in some circumstances, be required rather than permitted. The Confidentiality Advisory Group of the Health Research Authority will not usually authorise disclosures under regulation 5 to which the patient has objected. See the legal annex to this guidance for more detail on the regulations.

41. In Scotland, the Public Benefit and Privacy Panel for Health and Social Care scrutinises requests for access to some (but not all) NHS Scotland originated data. You may disclose personal information if the disclosure has been approved by the Public Benefit and Privacy Panel for Health and Social Care.

42. The Confidentiality Advisory Group (CAG) of the Health Research Authority publishes a range of guidance for CAG applicants, which you may find helpful. It is available at www.hra.nhs.uk.

43. Disclosure of the whole record may breach the principles of data protection law, as the full record may contain information that is excessive and not relevant for the purpose.

44. If any of the exceptions set out in paragraph 115(d) 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: www.gov.uk/government/collections/healthcare-practitioners-guidance-and-information-from-dwp.

45. 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.* For more details see the *Confidentiality: key legislation* factsheet which you can find on the our confidentiality guidance page at www.gmc-uk.org/guidance.

46. See also our guidance *Doctors' use of social media* (General Medical Council, 2013). You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

47. *Raising and acting on concerns about patient safety* (General Medical Council, 2012). See endnote 46 for the web address.

48. The GDPR defines a 'data controller' as: 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. Key definitions of terms in the *General Data Protection Regulation* are available on the website of the Information Commissioner's Office, at www.ico.org.uk.

49. The *Guide to data protection* is available on the website of the Information Commissioner's Office, at www.ico.org.uk.

50. This is contained in the *Guide to data protection*; see endnote 49.

51. The Information Commissioner's Office publishes technical guidance. NHS Digital formerly known as Health and Social Care Information Centre in England publishes good practice guidelines on technology-specific areas of information security and information governance: www.digital.nhs.uk. 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: www.igt.hscic. gov.uk. In Scotland, guidance and information governance standards are collected on the Knowledge Network: www.knowledge. scot.nhs.uk. 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 can check their compliance using the Welsh GMP Toolkit: www.wales.nhs.uk.

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

53. Schedules of minimum retention periods for different types of records are given in *The Records Management Code of Practice for Health and Social Care* (Information Governance Alliance, 2016); *Records Management: NHS Code of Practice (Scotland)* (Scottish Government, 2008); *Welsh Health Circular (2000)* 71: *For The Record* (The National Assembly for Wales, 2000) and *Good Management, Good Records* (Department of Health, Social Services and Public Safety, 2005). 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.

54. Article 15 of the *General Data Protection Regulation* gives patients the right to access their personal information, although exemptions apply in certain circumstances. Most exemptions are contained in the *Data Protection Act 2018*. 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 Office technical guidance, *Dealing with subject access requests involving other people's information* (Information Commissioner's Office, 2014).

55. The Scottish Government and NHS Scotland have published *Using email in NHS Scotland: A Good Practice Guide* (2014). The Professional Record Standards Body and the Health and Social Care Information Centre have published *Faster, better, safer communications: Using email in health and social care (in England)* (2015).

56. 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.

57. See paragraph 73 of *Good medical practice* (General Medical Council, 2013) and paragraph 22 of our explanatory guidance *Acting as a witness in legal proceedings* (General Medical Council, 2013). You can find all our guidance on professional standards and ethics at www.gmc-uk.org/guidance.

58. See endnote 39 for references to statutory duties of candour.

59. 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.

60. See endnote 36 for a description of clinical outcome review programmes.

61. 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 of 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*.

Email: **gmc@gmc-uk.org**

Website: **www.gmc-uk.org**

Telephone: **0161 923 6602**

General Medical Council, 3 Hardman Street, Manchester M3 3AW

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**.

ISBN: 978-0-901458-94-0

The GMC is a charity registered in England and Wales (1089278) and Scotland (SC037750)

Code: GMC/CON/0418

General Medical Council