Executive summary
At its closed session on 9 November 2016, Council considered the revised Confidentiality guidance and associated explanatory statements, and the process by which they were reviewed. Council agreed that:

a. The process had provided sufficient and appropriate opportunities for key interest groups to inform the decisions about content and format.

b. The executive had carried out its delegated responsibilities effectively.

c. The guidance should be brought back to the Council meeting on 14 December to be formally approved for publication in January 2017.

Council also considered and offered views on the ways in which we plan to help doctors and others to navigate the guidance and put the principles into practice.

Recommendations
Council is asked to:


b. Approve the explanatory statement on gun shots and knife wounds, at Annex C.

c. Note the plans for launch and implementation of the guidance, at Annex D, which have been updated to reflect the discussion at the closed session in November 2016.
Background

1 Since 2014 we have been undertaking a project to review our 2009 *Confidentiality* guidance and the associated explanatory guidance and materials, to ensure that they remain compatible with the law and relevant to medical practice.

2 Between November 2015 and February 2016 we carried out a consultation on the revised *Confidentiality* guidance, the development of which was overseen by an expert, externally chaired, task and finish group, with clinical, legal and lay representation. The consultation responses were analysed in March 2016 and proposals for redrafting the guidance were considered by the task and finish group at meetings in April and May, and by email circulation in June 2016. The guidance then was reviewed by legal counsel in July and August, and edited for tone of voice in August 2016. The text of the guidance was agreed by the Strategy and Policy Board at its meeting on 6 October 2016, in accordance with the Schedule of Authority which delegates functions in relation to the provision of advice to the profession to the Registrar.

3 At its closed session on 9 November 2016, Council considered the revised guidance and the process by which it was developed. They agreed that the consultation process had provided sufficient and appropriate opportunities for key interest groups to inform decisions about the content and format of the new guidance, and that the executive had carried out its delegated responsibilities effectively.

4 Council agreed that the guidance should be brought back to the meeting on 14 December 2016 to approve publication in January 2017.

5 The core guidance is at Annex A, and the explanatory statements are at Annex B and Annex C.

Launch and implementation

6 The guidance will be published in January 2017, and will come into effect three months later.

7 The existing guidance and associated materials will remain current until the new version comes into effect. To reduce the possibility of confusion about the status of the new guidance, we will publish only pdf and hard copies in January 2017, and will make them available on our ‘News and consultations’ and ‘Confidentiality review’ pages rather than our guidance pages.

8 The priority for our communications at launch will be to raise awareness of the new guidance with doctors, as well as the wide range of organisations that are likely to quote from our current guidance. We will also tell the story the journey of how we developed the guidance and highlight what has changed.

9 The new guidance has been designed to be accessed in interactive digital, as well as paper, formats in line with the principles of our ‘digital first’ strategy. When it comes into
effect in April 2017 it will be added to the GMC app and published in e-book format. At this point a suite of supporting resources (including case studies and short guides) will also be launched to support doctors in applying the guidance in practice. There is more detail on launch and implementation plans at Annex D.

Next steps

10 We will finalise the communications plan for the publication of the guidance in January, and continue to develop the case studies and other resources to support doctors’ awareness, understanding and use of the guidance when it comes into force the following April 2017.
Confidentiality: good practice in handling patient information
Confidentiality:

good practice in handling patient information
[Duties of a doctor to be included on inside cover]
Confidentiality: good practice in handling patient information

This guidance has been edited for plain English.

Published January 2017.

Comes into effect 25 April 2017.

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this guidance</td>
<td>6</td>
</tr>
<tr>
<td>Other materials available</td>
<td>7</td>
</tr>
<tr>
<td>Ethical and legal duties of confidentiality</td>
<td>8</td>
</tr>
<tr>
<td>Acting within the law</td>
<td>8</td>
</tr>
<tr>
<td>The main principles of this guidance</td>
<td>10</td>
</tr>
<tr>
<td>Disclosing patients’ personal information: a framework</td>
<td>11</td>
</tr>
<tr>
<td>When you can disclose personal information</td>
<td>11</td>
</tr>
<tr>
<td>Disclosing information with a patient’s consent</td>
<td>12</td>
</tr>
<tr>
<td>Disclosing information when a patient lacks the capacity to consent</td>
<td>13</td>
</tr>
<tr>
<td>Disclosures required or permitted by law</td>
<td>13</td>
</tr>
<tr>
<td>Disclosures approved under a legal process</td>
<td>14</td>
</tr>
<tr>
<td>Disclosures in the public interest</td>
<td>14</td>
</tr>
<tr>
<td>Disclosures prohibited by law</td>
<td>14</td>
</tr>
<tr>
<td>Flowchart</td>
<td>15</td>
</tr>
<tr>
<td>Using and disclosing patient information for direct care</td>
<td>16</td>
</tr>
<tr>
<td>Sharing information for direct care</td>
<td>16</td>
</tr>
<tr>
<td>Implied consent and sharing information for direct care</td>
<td>16</td>
</tr>
<tr>
<td>Patient objections to sharing information for direct care</td>
<td>17</td>
</tr>
<tr>
<td>If a patient cannot be informed</td>
<td>17</td>
</tr>
<tr>
<td>Sharing information with those close to the patient</td>
<td>18</td>
</tr>
<tr>
<td>Establishing what the patient wants</td>
<td>18</td>
</tr>
<tr>
<td>Abiding by the patient’s wishes</td>
<td>18</td>
</tr>
<tr>
<td>Listening to those close to the patient</td>
<td>19</td>
</tr>
<tr>
<td>Disclosures about patients who lack capacity to consent</td>
<td>19</td>
</tr>
<tr>
<td>Considering the disclosure</td>
<td>20</td>
</tr>
<tr>
<td>If a patient who lacks capacity asks you not to disclose</td>
<td>21</td>
</tr>
<tr>
<td>Disclosures for the protection of patients and others</td>
<td>22</td>
</tr>
<tr>
<td>Disclosing information about children who may be at risk of harm</td>
<td>22</td>
</tr>
</tbody>
</table>
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:

- disclosures to support the direct care of an individual patient
- disclosures for the protection of patients and others
- 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.

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

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 guardian¹ or equivalent, 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:

- patients' fitness to drive and reporting concerns to the DVLA or DVA
- disclosing information about serious communicable diseases
- disclosing information for employment, insurance and similar purposes
- disclosing information for education and training
- reporting gunshot and knife wounds
- 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, we summarise some key elements of the relevant law, including the requirements of the common law, the *Data Protection Act 1998* and the *Human Rights Act*.
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.

If you are not sure how the law applies in a particular situation, you should consult a Caldicott or data guardian, 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.¹

- **Use the minimum necessary personal information.** Use anonymised information if it is practicable to do so and if it will serve the purpose.

- **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.

- **Be aware of your responsibilities.** Develop and maintain an understanding of information governance that is appropriate to your role.

- **Comply with the law.** Be satisfied that you are handling personal information lawfully.

- **Share relevant information for direct care** as long as you are satisfied the patient can easily access information that explains how their information will be used and that they have the right to object, and you have no reason to believe the patient has objected.

- **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.

- **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.

- **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 apply.

a The patient consents, whether implicitly for the sake of their own care or for local clinical audit, or explicitly for other purposes (see paragraphs 13–15).

b The disclosure is of overall benefit\(^4\) to a patient who lacks the capacity to consent (see paragraphs 41–59).

c The disclosure is required by law (see paragraphs 17–19), or the disclosure is permitted or has been approved under a statutory process which sets aside the common law duty of confidentiality (see paragraphs 20–21).

d 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 information will be used for their direct 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 direct 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.\(^5\)
When you are satisfied that information should be disclosed, you should act promptly to disclose all relevant information.

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 or detection of serious crime.

**Disclosing information with a patient’s consent**

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

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

- **Implied consent** refers to circumstances in which it would be reasonable to infer that the patient agrees to the use of the information, even though this has not been directly expressed.

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:

- the disclosure is required by law (see paragraphs 17–19)

- you are satisfied that informed consent has already been obtained by a suitable person

- 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)

- you have reason to believe that seeking consent would put you or others at risk of serious harm
seeking consent would be likely to undermine the purpose of the disclosure, for example by prejudicing the prevention or detection of serious crime

- action must be taken quickly, for example in the detection or control of outbreaks of some communicable diseases where there is insufficient time to contact the patient
- seeking consent is not feasible given the number or age of records, or the likely traceability of patients.

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). Examples of legal requirements to disclose information about patients are given in the legal annex.

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 or detection of serious crime.

19 Laws and regulations sometimes permit, but do not require, the disclosure of personal information. 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 direct 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 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.
As a rule, personal information about patients should not be disclosed unless it is necessary. The following 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. 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. 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).

28 The usual basis for sharing information for direct 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.
You are satisfied that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect.

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 direct care

If a patient objects to particular personal information being shared for their direct care, you should not disclose the information unless it would be justified in the public interest, 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.

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

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.
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

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

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.

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

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).
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

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.

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. You should also take care not to disclose confidential information unintentionally – for example, by confirming or denying the person’s perceptions about the patient’s health.

Disclosures about patients who lack capacity to consent

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.

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.
We give detailed advice on assessing a patient’s mental capacity in our guidance on 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.

Considering the disclosure

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.

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.

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.14

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 and the legal annex).

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

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

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

Disclosing information about adults who may be at risk of harm

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

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. 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.
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**

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.

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**

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

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.\textsuperscript{18,19} 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.\textsuperscript{20} 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.\textsuperscript{21}

**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 it is not safe or practicable to do so (see paragraph 14), or the information is required by law. 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.\textsuperscript{22}

64 If it is not practicable 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 public and the patient’s 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, or has been diagnosed with a serious communicable disease, or poses a serious risk to others through being unfit for work.

67 When deciding whether the public interest in disclosing information outweighs patients’ 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
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. You should inform the patient before disclosing the information, if it is practicable and safe to do so, even if you intend to disclose without their consent.

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.

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

Responding to requests for information

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). 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:

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

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

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.

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.

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

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

- The disclosure is required by law, including by the courts (see paragraphs 87–94).
- The patient has given explicit consent (see paragraph 95).
- The disclosure is approved through a statutory process which sets aside the common law duty of confidentiality (see paragraphs 103–105).
- 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 (ICO) anonymisation code of practice 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. Simply removing the patient’s name, age, address or other personal identifiers is unlikely to be enough to anonymise information to this standard.

82 The 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 dataset disclosed into a secure and controlled environment could remain anonymous even though the same dataset could not be made publically available because of the likelihood of individuals being identified.

83 You should follow the ICO anonymisation code of practice, 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. You can find examples in the legal annex.

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 paragraphs 17–19.
Disclosing information to 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.
Consent

95 You should ask for consent to disclose personal information for purposes other than direct care\textsuperscript{34} 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\textsuperscript{35} and to contribute to clinical outcome review programmes.\textsuperscript{36} If an audit will be carried out by the team that provided care, or those working to support them, such as clinical audit staff, you may disclose personal information 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, you should explain why the information is needed and how this may benefit their own and others’ 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 the options open to them.

98 If a clinical audit will be carried out, but not by the team that provided care or those who 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). 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.

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. 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, or 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.

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 public and patients’ 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 patient (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 direct 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, 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.

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:

- handwritten notes
- electronic records
- correspondence between health professionals
- visual and audio recordings
- laboratory reports
- 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. 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 to 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 the Data Protection Act 1998**

125 The *Data Protection Act 1998* sets out the responsibilities of data controllers48 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).

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:

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

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 to their own records

Patients have a right to access to their own health records, subject to certain safeguards. You should respect, and help patients to exercise, their legal rights to have access to, or copies of, their health records. The Information Commissioner’s Office gives guidance on what fees you may charge. You should also follow our guidance on fees in Financial and commercial arrangements and conflicts of interest.

Communicating with patients

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.

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 and that you meet patients’ expectations about how they will receive information.

Disclosing information after a patient has died

Your duty of confidentiality continues after a patient has died.

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
- on death certificates, which you must complete honestly and fully
- when a person has a right of access to records under the Access to Health Records Act 1990 or the Access to Health Records (Northern Ireland) Order 1993, unless an exemption applies (see the legal annex)
- when disclosure is necessary to meet a statutory duty of candour.
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;

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 which 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 a 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, 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.

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 the 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:

- the patient consents
- it is required by law, or in response to a court order
- 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 Act 1998 (UK)

The Data Protection Act 1998 regulates the processing of personal data about living individuals in the UK. It sets out the responsibilities of data controllers when processing personal data as well as a number of rights for individuals, including rights of access to their information. The Information Commissioner (ICO) is the authority responsible for upholding information rights in the UK. Detailed guidance on complying with the Act is available on the website of the Information Commissioner’s Office: www.ico.org.uk.

The Act defines personal data as:

'data which relate to a living individual who can be identified

a from those data, or
b from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.'

ICO guidance also says ‘where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be “personal data”’.  

The Act defines a data controller as ‘a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed’. 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 Act is based around eight data protection principles, which state that personal data must:

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

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

patients’ information must not be processed in a way that breaches either statute or common law. For example, disclosing information would be a breach of the common law duty of confidentiality, it would also be unlawful under the Act
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 Schedule 2 (for all personal data) and Schedule 3 (for sensitive personal data) to the Act 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 Schedule 2 must be met. The conditions most likely to be relevant in medical practice are that:

the data subject has given consent (Schedule 2, paragraph 1)
the processing is necessary because of a legal obligation that applies to the data controller (except an obligation imposed by a contract) (Schedule 2, paragraph 3)
the processing is necessary to protect the vital interests of the data subject (Schedule 2, paragraph 4)
the processing is necessary for the exercise of functions of a public nature exercised in the public interest (Schedule 2, paragraph 5d)

the processing is necessary for the purposes of legitimate interests pursued by the data controller (Schedule 2, paragraph 6).

Where ‘sensitive personal data’ are being used, at least one of the conditions in Schedule 3 must also be met. Information on a patient’s health record is likely to be ‘sensitive personal data’ for the purposes of the Act. The conditions most likely to be relevant in medical practice are that:

- the data subject has given explicit consent (Schedule 3, paragraph 1)
- the processing is necessary to protect the vital interests of the data subject or another person in a case where consent cannot be obtained or has been unreasonably withheld (Schedule 3, paragraph 3)
- 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 confidence (Schedule 3, paragraph 8).

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

**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 website of the Information Commissioner’s Office:
www.ico.org.uk. Guidance about the *Freedom of Information (Scotland) Act 2002* is
available on the website of the Scottish Information Commissioner:
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 and agencies and health and social services bodies or providers’ premises and inspect and take
copies of records, subject to the protection of confidential information provided for in section 43.

**NHS Protect** has powers under the *National Health Service Act 2006* and the *National Health Service (Wales) Act 2006* to require the production of documents to prevent, detect and prosecute fraud in the NHS. The Department of Health (England) and Welsh Assembly Government have published codes of practice for the use of these powers. 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 Service 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 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: http://systems.hscic.gov.uk/infogov/iga.

**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, 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.


**Other laws that require or permit disclosures**

**Access to patient records and disclosures of reports**


These pieces of legislation provide rights of access to a deceased patient’s personal representative and any person who may have a claim arising out of a patient’s death. This is not a general right, however, and access should be limited to information of relevance to the claim. Access should be limited or refused if there is evidence that the patient would have expected that the information would not be disclosed to the applicant, if disclosure is likely to cause serious harm to anyone else, or if it would also disclose information about a third party (other than a healthcare professional involved in the deceased person’s care) who does not consent. Access must be refused to records that contain a note, made at the patient’s request, expressing that they did not wish access to be given on an application under the Act. These Acts only give access to records created on or after the date on which they came into force (November 1991 for England, Scotland and Wales; 30 May 1994 for Northern Ireland). Access must also be given to information recorded before these dates if this is necessary to make any later part of the records intelligible.

*Access to Medical Reports Act 1988* (England, Scotland and Wales) and *Access to Personal Files and Medical Reports (Northern Ireland) Order 1991*. 

www.gmc-uk.org
These pieces of legislation give patients the right to see medical reports written about them, for employment or insurance purposes, by a doctor who is or has been responsible for the clinical care of the individual. This includes the right to see reports written by the patient’s GP or by a specialist who has provided care. Patients have the right to ask the doctor to amend any part of the report that the patient considers to be incorrect or misleading, and to attach their disagreement to the report, or to withdraw their consent for the release of the information.

**Adult safeguarding and support**

*Adult Support and Protection (Scotland) Act 2007.*

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

*Care Act 2014* (England)

This Act requires ‘relevant partners’ to cooperate with local authorities making enquiries about adults at risk unless an exemption set out in the Act applies. Relevant partners include NHS trusts, foundation trusts and clinical commissioning groups in the local authority’s area. Certain persons or bodies must also give information to safeguarding adults boards, if they ask for the information to enable or assist the board to perform its functions. The explanatory notes to the Act make clear that individual doctors can be asked for information under this provision. You can read detailed guidance in the Care and Support Statutory Guidance.

*Carers (Scotland) Act 2016*

This Act places duties on local authorities to seek and take account of the views of carers when determining a cared for person’s needs. It also placed a duty on health boards to share information with carers about a cared for person who is being discharged from
hospital and to seek the views of the carers about the discharge and take account of those views. The Act is expected to come into force in 2017–18.

**Social Services and Well-being (Wales) Act 2014**

This Act requires ‘relevant partners’ (which include local health boards and NHS trusts in Wales) to tell local authorities if they have reasonable cause to suspect an adult is at risk of harm (whether or not they lack capacity to make the decision). The Act also requires relevant partners to cooperate with local authorities making enquiries about adults at risk, and certain persons or bodies to give information to adults safeguarding boards, unless an exemption set out in the Act applies.

**Mental capacity and mental health legislation**

**Adults with Incapacity (Scotland) Act 2000** and **Mental Capacity Act 2005** (England and Wales).

These pieces of legislation provide for information to be shared with anyone who is authorised to make decisions on behalf of, or who is appointed to support and represent, a patient who lacks capacity. This might be a welfare attorney, a court-appointed deputy or guardian or an independent mental capacity advocate. You can read detailed guidance in the *Adults with Incapacity (Scotland) Act 2000* codes of practice, and in the *Mental Capacity Act Code of Practice*. The main provisions of the **Mental Capacity Act (Northern Ireland) 2016** have not yet come into force.

**Mental Health Act 1983, Mental Health (Care and Treatment) (Scotland) Act 2003** and **Mental Health Northern Ireland Order (1986)**. These pieces of legislation provide for a number of situations in which confidential information about patients can be disclosed, even if the patient does not consent. You can find detailed guidance in the *Mental Health Act 1983: Code of Practice*; in the *Code of Practice* under the *Mental Health (Care & Treatment) (Scotland) Act 2003*; on the website of the Mental Welfare Commission for Scotland, see www.mwcscot.org.uk/the-law/mental-health-act; and in the *Guidelines on the use of the Mental Health (Northern Ireland) Order 1996*. The main provisions of the **Mental Capacity Act (Northern Ireland) 2016** have not yet come into force.
Public health and other mandatory notification schemes

Abortion Regulations 1991 (England and Wales) and Abortion (Scotland) Regulations 1991. A doctor who has carried out a termination of pregnancy must notify the appropriate chief medical officer of that fact within seven days of the termination. There is no equivalent legislation in Northern Ireland.

The Controlled Drugs (Supervision of Management and Use) Regulations 2013 (England and Scotland); The Controlled Drugs (Supervision of Management and Use) Regulations (Northern Ireland) 2009 (as amended) and The Controlled Drugs (Supervision of Management and Use) (Wales) Regulations 2008

Under these regulations, responsible bodies are required to cooperate with each other in relation to the handling of, and acting on, shared information relating to the management and use of controlled drugs. As far as possible, information that identifies patients should be removed before disclosure, but it may be necessary for identifiable information to be disclosed in some circumstances, with consent if practicable. Further guidance is provided by the UK Department of Health for the regulations in England and Scotland: www.gov.uk/government/uploads/system/uploads/attachment_data/file/214915/15-02-2013-controlled-drugs-regulation-information.pdf; by the Department of Health Northern Ireland: www.health-ni.gov.uk/publications/guidance-safe-management-and-use-controlled-drugs; and by Healthcare Inspectorate Wales: www.hiw.org.uk/controlled-drugs.


Registered doctors in each of the UK countries have statutory duties to notify an appropriate person or body of suspected cases of certain infectious diseases. In England, Scotland and Wales, doctors must also notify cases of other infections or of contamination which they believe present, or could present, a significant risk to human health. Detailed guidance has been published by Public Health England: www.gov.uk/government/collections/notifications-of-infectious-diseases-noids#guidance; the Scottish Government: www.gov.scot/Topics/Health/Policy/Public-Health-
Prevention, detection and prosecution of crime

Crime and Disorder Act 1998 (UK)

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

Criminal Law Act (Northern Ireland) 1967

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

Road Traffic Act 1988 (England, Scotland and Wales) and Road Traffic (Northern Ireland Order) 1981

In certain circumstances, all citizens (including doctors) must give the police, on request, any information that may identify a driver alleged to have committed a traffic offence.

Terrorism Act 2000 (UK)

Under section 38B of this Act, it is a criminal offence for a person to fail to disclose information to the police that they know or believe might be relevant in preventing an act of terrorism or securing the arrest, prosecution or conviction of a person for a terrorist act. Even if the threshold for a disclosure required by law isn’t met, disclosure may still be justified in the public interest if there are clear grounds for believing that it will protect a specific person or people – or the public more broadly – from risk of death or serious
harm. The UK Department of Health has issued guidance on the ‘prevent duty’ for healthcare professionals that sets out the types of behaviour doctors should be aware of.

Building Partnerships, Staying Safe: The health sector contribution to HM Government’s Prevent strategy: guidance for healthcare workers (Department of Health, 2011) reassures doctors that they are not expected to take on a surveillance role, but sets out the sorts of steps they might take if they are concerned that a patient may be involved in, or at risk of being drawn into, terrorist-related activity.

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

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

2 In 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 the Data Protection Act 1998. See the legal annex to this guidance for more information.

6 We give detailed advice on consent in our guidance Consent: doctors and patients making decisions together (General Medical Council, 2008). You can find all GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

7 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. See paragraph 115 of this guidance.

8 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.’

9 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.

10 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.

11 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.

12 Patients are also entitled to access their health records under the Data Protection Act 1998. See endnote 54.

13 See the Adults with Incapacity (Scotland) Act 2000 and the Mental Capacity Act 2005 and their respective codes of practice. 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.

14 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.

15 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.

16 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. See endnote 15 for the web address.

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

18 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.

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

20 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).

21 See “The duties of a doctor registered with the General Medical Council” at the front of this guidance.

22 There is no agreed definition of ‘serious crime’. The Confidentiality: NHS Code of Practice Supplementary Guidance on 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); 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). NHS Protect has published *Not part of the job* (NHS Protect, 2012), which gives guidance to NHS staff on reporting assaults and violent incidents at work.

23 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.

24 See our explanatory guidance *Confidentiality: disclosing information about serious communicable diseases*. See endnote 23 for the web address.

25 See our explanatory guidance *Confidentiality: disclosing information for employment, insurance and similar purposes*. See endnote 23 for the web address.

26 You should consider the assessment of risk posed by patients made by other professionals and by groups established for that purpose, but you must make your own assessment and decision as to whether disclosure is justified. Your assessment of risk is a matter of professional judgement in which an offender’s past behaviour will be a factor. The Royal College of Psychiatrists publishes guidance for psychiatrists about sharing information in the context of public protection, including participation in multi-agency public protection arrangements (MAPPA) and panels. You can find this in *Good Psychiatric Practice: Confidentiality and Information Sharing* (Royal College of Psychiatrists, second edition, 2010).

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

28 See endnote 2 for the definition of ‘personal information’ in this guidance.


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* in England and NHS Scotland’s *The Charter of Patient Rights and Responsibilities* both set out the rights of a patient to object to how their information is used. Under the *Data Protection Act 1998*, a data subject has a right to object to processing if it causes unwarranted and substantial damage or distress. For more information, see the *Guide to Data Protection* on the ICO website, 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, www.lawscot.org.uk.
34 See endnote 9 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: 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) Directions 2005 and Code of Practice (Scottish Executive Health Department, 2005); 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 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) NHSScotland 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 of the Health Research Authority has published a document which clarifies how the group interprets the term ‘reasonably practicable alternative’ to using confidential
information without consent, which you may find helpful. It is available at:

43 Disclosure of the whole record may breach the principles of the Data Protection Act 1998, 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 120(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. See the legal annex to this guidance for more details.

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 Act defines a ‘data controller’ as a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. Key definitions of terms in the Data Protection Act 1998 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. The Health and Social Care Information Centre in England publishes good practice guidelines on technology-specific areas of information security and information governance: http://systems.hscic.gov.uk/infogov/security/infrasec/gpg. 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/ig.aspx. 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: www.wales.nhs.uk/sites3/home.cfm?orgid=950. GPs are required to assess their compliance with the Information Security Management System (ISMS) framework on an annual basis using the Online ISMS Toolkit: www.wales.nhs.uk/sites3/page.cfm?orgid=950&pid=51811.

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 (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.

Section 7 of the Data Protection Act 1998 gives patients the right to access their personal information, although exemptions apply in certain circumstances. For example, an exemption applies if providing subject access to information about an individual’s physical or mental health or condition would be likely to cause serious harm to them or to another person’s physical or mental health or condition. You also do not have to supply a patient with information about another person or that identifies another person as the source of the information, unless that other person consents or it is reasonable in the circumstances to supply the information without their consent. See the Information Commissioner’s technical guidance, Dealing with subject access requests involving other people’s information (Information Commissioner’s Office, 2014).


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.

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 GMC guidance on professional standards and ethics at www.gmc-uk.org/guidance.

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.

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

You should contact your organisation’s approved place of deposit or The National Archives, the Public Record Office of Northern Ireland or the National Archives for Scotland for further advice about storage of, and access to, archives of records of ongoing research or historical value. Health records of deceased patients are exempt from the Freedom of Information (Scotland) Act 2002.
M11 - Confidentiality guidance

M11 - Annex B

Explanatory statements

1. Patients’ fitness to drive and reporting concerns to the DVLA or DVA
2. Disclosing information about serious communicable diseases
3. Disclosing information for employment, insurance and similar purposes
4. Disclosing information for education and training purposes
5. Responding to criticism in the media
Confidentiality: patients’ fitness to drive and reporting concerns to the DVLA or DVA

1 In our guidance Confidentiality we say:

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

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.

62 You should ask for a patient’s consent to disclose information for the protection of others unless it is not safe or practicable to do so,¹ or the information is required by law. You should consider any reasons given for refusal.

64 If it is not practicable 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 public and the patient’s interest in keeping the information confidential.

68 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. You should inform the patient before disclosing the information, if it is
practicable and safe to do so, even if you intend to disclose without their consent.

About this guidance

2 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. This explanatory guidance sets out the steps doctors should take if a patient’s failure or refusal to stop driving exposes others to a risk of death or serious harm.

Fitness to drive: doctors’ and patients’ responsibilities

3 The Driver and Vehicle and Licensing Agency (DVLA) in England, Scotland and Wales and the Driver and Vehicle Agency (DVA) in Northern Ireland are legally responsible for deciding if a person is medically unfit to drive. This means they need to know if a person holding a driving licence has a condition or is undergoing treatment that may now, or in the future, affect their safety as a driver.

4 The driver is legally responsible for telling the DVLA or DVA about any such condition or treatment. Doctors should therefore alert patients to conditions and treatments that might affect their ability to drive and remind them of their duty to tell the appropriate agency. Doctors may, however, need to make a decision about whether to disclose relevant information without consent to the DVLA or DVA in the public interest if a patient is unfit to drive but continues to do so.

Assessing a patient’s fitness to drive

5 When diagnosing a patient’s condition, or providing or arranging treatment, you should consider whether the condition or treatment may affect their ability to drive safely. You should:

• refer to the DVLA’s guidance Assessing fitness to drive – a guide for medical professionals, which includes information about disorders and conditions that can impair a patient’s fitness to drive
• seek the advice of an experienced colleague or the DVLA’s or DVA’s medical adviser if you are not sure whether a condition or treatment might affect a patient’s fitness to drive.
Reporting concerns to the DVLA or DVA

6 If a patient has a condition or is undergoing treatment that could impair their fitness to drive, you should:

a explain this to the patient and tell them that they have a legal duty to inform the DVLA or DVA

b tell the patient that you may be obliged to disclose relevant medical information about them, in confidence, to the DVLA or DVA if they continue to drive when they are not fit to do so

c make a note of any advice you have given to a patient about their fitness to drive in their medical record.

7 If a patient is incapable of understanding this advice – for example, because of dementia – you should inform the DVLA or DVA as soon as practicable.

8 If a patient refuses to accept the diagnosis, or the effect of the condition or treatment on their ability to drive, you can suggest that they seek a second opinion, and help arrange for them to do so. You should advise the patient not to drive in the meantime. As long as the patient agrees, you may discuss your concerns with their relatives, friends or carers.

9 If you become aware that a patient is continuing to drive when they may not be fit to do so, you should make every reasonable effort to persuade them to stop. If you do not manage to persuade the patient to stop driving, or you discover that they are continuing to drive against your advice, you should consider whether the patient’s refusal to stop driving leaves others exposed to a risk of death or serious harm. If you believe that it does, you should contact the DVLA or DVA promptly and disclose any relevant medical information, in confidence, to the medical adviser.

10 Before contacting the DVLA or DVA, you should try to inform the patient of your intention to disclose personal information. If the patient objects to the disclosure, you should consider any reasons they give for objecting. If you decide to contact the DVLA
or DVA you should tell your patient in writing once you have done so, and make a note on the patient’s record.

Responding to requests for information from the DVLA or the DVA

11 If you agree to prepare a report or complete or sign a document to assist the DVLA’s or the DVA’s assessment of a patient’s fitness to drive, you should do so without unreasonable delay.

Endnotes

1 We give examples of when it might not be practicable to seek consent in paragraph 14 of Confidentiality. You can find all of our guidance online at www.gmc-uk.org/guidance.

2 See ‘The duties of a doctor registered with the General Medical Council’ in Good medical practice, which you can find at www.gmc-uk.org/guidance.

3 The principles in this guidance also apply to drivers and pilots of other kinds of regulated transport, including by rail, water and air, although such individuals are likely to undergo medical assessment as part of the relevant licensing or certificating process. If you are concerned that a patient who holds a private or commercial pilot licence may be medically unfit to fly an aircraft, you can contact the UK Civil Aviation Authority’s medical department on 01293 573 700 or at medicalweb@caa.co.uk for confidential advice. For advice about a seafarer, you can contact the Maritime and Coastal Agency health and safety branch for advice at seafarers.h&s@mcoa.gov.uk. If you are concerned that a train driver’s medical condition or treatment may make them unfit to drive a train, the advice from the Office of Rail and Road (ORR) is to make contact with the patient’s HR department in the first instance. The ORR can provide contact details for HR departments in Great Britain if you know the name of the employer.

4 You can find this at www.gov.uk/government/publications/assessing-fitness-to-drive-a-guide-for-medical-professionals.

5 You can contact the DVLA’s medical advisers on 01792 782 337 or at medadviser@dvla.gsi.gov.uk, and the DVA on 028 703 41369.
Confidentiality: disclosing information about serious communicable diseases

1 In our guidance Confidentiality we say:

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

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.

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 or detection of serious crime.

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

64 If it is not practicable 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 public and the patient’s interest in keeping the information confidential.
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. You should inform the patient before disclosing the information, if it is practicable and safe to do so, even if you intend to disclose without their consent.

About this guidance

2 Confidentiality is important to all patients and all patients are entitled to good standards of care, regardless of their status, what disease they might have, or how they acquired it. Those who have, or may have, a serious communicable disease might be particularly concerned about their privacy. This explanatory guidance sets out how the general principles in our guidance Confidentiality apply when doctors are accessing, using, or disclosing information about the infection status of patients who have serious communicable diseases.

Protecting information against improper disclosure

3 You should make sure that information you hold or control about a patient’s infection status is at all times effectively protected against improper disclosure. If you disclose information about a patient’s infection status, you must keep disclosures to the minimum necessary for the purpose.

Control and surveillance of serious communicable diseases

4 You must pass information about notifiable diseases to the relevant authorities for communicable disease control and surveillance. Different diseases are notifiable in different UK countries and the reporting arrangements differ. You should follow the arrangements where you work. You should disclose anonymised information if practicable and as long as it will serve the purpose.

Protecting patients from risks posed by your health or your colleagues’ health

5 Good medical practice says:
If you know or suspect that you have a serious condition that you could pass on to patients, or if your judgement or performance could be affected by a condition or its treatment, you must consult a suitably qualified colleague. You must follow their advice about any changes to your practice they consider necessary. You must not rely on your own assessment of the risk to patients.

You should be immunised against common serious communicable diseases (unless otherwise contraindicated).

You should follow our guidance *Raising and acting on concerns about patient safety* if you are concerned that a colleague who has a serious communicable disease is practising, or has practised, in a way that puts patients at risk of infection. You should inform your colleague before passing the information on, as long as it is practicable and safe to do so.

**Disclosing information about patients who are diagnosed with a serious communicable disease to those providing direct care**

Most patients understand and expect that relevant information must be shared within the direct care team to provide their care. If a patient objects to disclosure of personal information that you are convinced is essential to provide them with safe care, you should follow the guidance at paragraphs 30 and 31 of *Confidentiality*. If the patient does not have capacity to make the decision, you can disclose information if it is in their overall benefit, in line with the guidance at paragraphs 48 and 49 of *Confidentiality*.

If a patient who has been diagnosed with a serious communicable disease refuses to allow you to tell others providing their care about their infection status, and you believe that failing to disclose the information will put healthcare workers or other patients at risk of infection, you should explain to the patient the potential consequences of their decision and consider with the patient whether any compromise can be reached.
Like everyone else, healthcare workers are entitled to protection from risks of serious harm. But disclosure of information about a patient’s infection status without consent is unlikely to be justified if it would make no difference to the risk of transmission - for example if the risk is likely to be managed through the use of universal precautions that are already in place. If the patient continues to refuse to allow you to tell other members of the healthcare team about their infection status, you must abide by their wishes unless you consider that disclosing the information is necessary to protect healthcare workers or other patients from a risk of death or serious harm.

**Disclosing information in response to injuries to colleagues and others**

If a colleague, police officer or anyone else suffers a needlestick or similar injury involving a patient who has, or may have, a serious communicable disease, you should make sure that a risk assessment is made urgently by an appropriately qualified colleague. Post-exposure prophylaxis should be offered in accordance with that risk assessment, depending on the type of body fluid or substance involved and the route and severity of the exposure.

You should ask for the patient’s consent to disclose their infection status after other people have been exposed to a serious communicable disease. If the patient cannot be persuaded to consent to disclosure, or if it is not safe or practicable to ask for their consent, you may disclose information if it is justified in the public interest. This could be, for example, if the information is needed for decisions about the continued appropriateness of post-exposure prophylaxis.

**Informing people at risk of infection from serious communicable disease**

You should explain to patients who have serious communicable diseases how they can protect others from infection, including from sexually transmitted diseases. This includes the practical measures they can take to avoid transmission, and the importance of informing people with whom they have sexual contact about the risk of sexual transmission of serious communicable diseases.

You may disclose information to a person who has close contact with a patient who has a serious communicable disease if you have reason to think that:
a. the person is at risk of infection that is likely to result in serious harm
b. the patient has not informed them and cannot be persuaded to do so.

14 If you believe that an adult who is at risk of infection lacks capacity to understand this information, and is at risk of serious harm, you must give relevant information promptly to an appropriate responsible person or authority, unless it is not of overall benefit to the patient to do so (see paragraphs 55 and 56 of Confidentiality).

15 You should tell the patient before you disclose the information if it is practicable and safe to do so. When you are tracing and notifying people, you should not disclose the identity of the patient, if practicable. You must be prepared to justify a decision to disclose personal information without consent. 

**Disclosing information when children and young people are at risk of a serious communicable disease**

16 Most patients with a serious communicable disease who are parents of, or care for, children will do all they can to protect the children from the risk of infection or the effects of the disease. You should make sure the patient understands the information and advice you give them, which you should tailor to their needs. You should do all you reasonably can to support them in caring for themselves and in protecting their children.

17 You should explain to a patient with a serious communicable disease the importance of testing any children who may already be infected, including children without symptoms and young people who might have been vertically infected with a blood-borne virus.

18 If you are concerned that a child is at risk of serious harm because their parents cannot be persuaded to protect them from the risk of infection, or because they refuse to allow the child to be tested, you should treat it as a safeguarding concern and follow the advice in our guidance Protecting children and young people: the responsibilities of all doctors. 

www.gmc-uk.org
Recording serious communicable diseases on death certificates

19 If a serious communicable disease has contributed to the cause of death, you must record this on the patient’s death certificate.

Endnotes

1 We give examples of when it might not be practicable to seek consent in paragraph 14 of Confidentiality. You can find all of our guidance online at www.gmc-uk.org/guidance.

2 In this guidance, the term ‘serious communicable disease’ applies to any disease that can be transmitted from human to human and that can result in death or serious illness. It particularly applies to, but is not limited to, HIV, tuberculosis, and hepatitis B and C.

3 You can get advice from the Health Protection Agency in England, Public Health Wales, Communicable Disease Surveillance Centre in Northern Ireland and Health Protection Scotland.

4 Good medical practice (General Medical Council, 2013). You can find all of our guidance online at www.gmc-uk.org/guidance.


6 Universal precautions, otherwise known as standard infection control precautions, are the basic infection prevention and control measures necessary to reduce the risk of transmitting infectious agents. Guidance on infection control is provided by Health Protection Scotland, NHS Wales, DHSSPS Northern Ireland and the Department of Health in England.


8 The NHS (Venereal Diseases) Regulations 1974, The NHS Trusts (Venereal Diseases) Directions 1991 and The NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000 state that various NHS bodies in England and Wales must ‘take all necessary steps to secure that any information capable of identifying an individual… with respect to persons examined or treated for any sexually transmitted disease shall not be disclosed except – (a) for the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof, and (b) for the purpose of such treatment and prevention’. There are different interpretations of the regulations and directions, and concerns about their compatibility with the European Convention on Human Rights. In particular, there have been concerns that a strict interpretation would prevent the disclosure of relevant information, except to other doctors or those working under their supervision, even with the patient’s consent or to known sexual contacts in the public interest. Our view is that the regulations and directions do not preclude disclosure if it would otherwise be lawful at common law, for example with the patient’s consent or in the public interest without consent.

9 See also our case study about a parent who refuses to allow her daughter to be tested for HIV, available at www.gmc-uk.org/guidance/ethical_guidance/13561.asp.
Confidentiality: disclosing information for employment, insurance and similar purposes

1 In our guidance Confidentiality we say:

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, 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.¹

About this guidance

2 One of the core duties of a doctor is to make the care of your patient your first
concern.² There are, however, many circumstances in which you might be asked to
disclose information from existing records or after examining a patient, and in which
you face dual obligations. By this we mean that you have obligations both to the
patient and to the person or organisation that has requested the information.

3 This explanatory guidance sets out how the general principles in our guidance
Confidentiality apply when patient information is being disclosed in these
circumstances. The guidance applies to disclosure of information obtained directly from
a patient, or from a patient's medical record, or from another health professional. It
does not apply if your opinions are based solely on information provided by the person
or body that is commissioning the opinion.

When do dual obligations arise?

4 Usually, dual obligations arise when a doctor works for, is contracted by, or otherwise
provides services to:

• a patient’s employer (as an occupational health doctor)
• an insurance company
• an agency assessing a claimant’s entitlement to benefits
• the police (as a police surgeon)
• the armed forces
• the prison service
• a sports team or association.³

5 Alternatively, a person or organisation you have previously had no direct relationship
with, such as your patient’s employer or insurance company, might ask you to provide
a medical report or information about a patient. You might be offered payment for your own or your staff’s time and effort, giving rise to an obligation in addition to the one you have to your patient.⁴

**How much information should you disclose?**

6 You should only disclose information that is relevant to the request, which means you should not usually disclose a patient’s whole record.⁵ There are two exceptions to this general rule.

- **Benefit claims:** the patient’s whole record may be relevant to some benefits paid by government departments or agencies.⁶

- **Legal processes:** a solicitor may need to see their client’s whole record to assess which parts are relevant, for example to personal injury claims. If the claim goes ahead, the person against whom the claim is made may ask for copies of important documents, which could include records containing the patient’s medical history. Under court rules in England and Wales, they can see the patient’s whole record and the solicitor should explain this to the patient. In Northern Ireland and Scotland, you should disclose your patient’s record in accordance with their wishes or as ordered by a court.⁷

**Writing reports**

7 When writing a report⁸ you must:

- **a** make sure it is not false or misleading – you must take reasonable steps to check the information in the report is correct, and you must not deliberately leave out relevant information

- **b** restrict the report to areas in which you have direct experience or relevant knowledge

- **c** make sure any opinion you include is balanced, and be able to state the facts or assumptions on which it is based.

**Disclosing a report about a patient**

8 You do not need to ask for separate consent to release a report following an examination as long as you are satisfied that the patient has given informed consent
both for the examination and for the release of any subsequent reports (see paragraph 115 of *Confidentiality*, which is reproduced at the top of this statement).

9 You should, however, usually 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.\(^9\)

10 If a patient asks you to amend a report, you should correct any errors of fact and any opinion that is based on errors of fact. You should not remove information, opinion or advice if you believe the report would be false or misleading as a result.

11 If a patient withdraws consent for the report to be disclosed, it may be appropriate for you to tell the patient that their decision may lead to adverse consequences for them. For example, the absence of occupational health information could disadvantage the patient in negotiations with their employer. You must, however, respect the patient’s wishes unless the disclosure is required by law (see paragraph 14) or can be justified in the public interest (see paragraph 15).

12 If a patient withdraws consent for a report to be disclosed, or fails to attend an appointment, you can let the report commissioner know but you should not disclose any further information.

13 When you are satisfied that a report should be disclosed, you should complete and send the report without unreasonable delay.

**Disclosures required by law**

14 You must disclose information if it is required by law or by the courts. If a disclosure is required by law, you should follow the guidance at paragraphs 87–94 of *Confidentiality*. If you are not sure whether a disclosure is required by law, you should ask the person or body requesting the information to identify the legal basis, or seek independent legal advice.
Disclosures in the public interest

15 Disclosing personal information about a patient without consent may be justified in the public interest if failure to do so may expose others to a risk of death or serious harm. This could arise, for example, if a patient may pose a serious risk to others through being unfit for work. If you think that a disclosure may be justified in the public interest you should follow the guidance at paragraphs 63–70 of Confidentiality.

Endnotes

1 You can find Confidentiality, and the rest of our guidance, online at www.gmc-uk.org/guidance.

2 The term ‘patient’ in this guidance refers to employees, clients, claimants, athletes and anyone else whose personal information you hold or have access to, whether or not you care for them in a traditional therapeutic relationship.

3 Doctors might provide their services to professional sports clubs (where the dual obligation is to both the patient and the club, which is very similar to the dual obligation of an occupational health doctor) or to associations (where the dual obligation is both to the patient and to a governing body or team of selectors).

4 This guidance is not intended for doctors who act as expert witnesses. We give specific guidance in Acting as a witness in legal proceedings, which you can find at www.gmc-uk.org/guidance.

5 Disclosure of the whole record may breach the principles of the Data Protection Act 1998, as the full record may contain information that is excessive and not relevant for the purpose. The Information Commissioner’s Office (ICO) has advised that it is not appropriate for insurance companies to obtain medical records using patients’ subject access requests. The Access to Medical Reports Act 1988 gives insurance companies a clear and established legal route to access medical information, while safeguarding patients’ rights. You can find the ICO statement at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/07/insurers-using-subject-access-requests-to-see-medical-information/.


7 The Law Society and British Medical Association jointly publish model consent forms authorising the release of health records to solicitors under the Data Protection Act 1998. The forms include notes for clients, solicitors and medical records controllers. You can find them at www.bma.org.uk/support-at-work/ethics/confidentiality-and-health-records.

8 See Good medical practice, paragraphs 71–74, which you can find at www.gmc-uk.org/guidance.

9 Under the Access to Medical Reports Act 1988, patients are entitled to see a report that has been written about them for employment or insurance purposes by a doctor who is or has been responsible for the clinical care of the individual before it is sent, unless exceptions apply. Patients have the right to ask the doctor to amend any part of the report that the patient considers to be incorrect or misleading, and to attach their
disagreement to the report, or to withdraw their consent for the release of the information. These provisions do not apply to reports for benefits purposes. If the patient has no legal right to see the report before it is sent, you should follow the guidance in paragraph 115(d) of Confidentiality, which is reproduced at the start of this explanatory guidance. If any of the exceptions set out in paragraph 115(d) apply, you should still disclose as much of the report as you can.
Confidentiality: disclosing information for education and training purposes

1  In our guidance *Confidentiality* we say:

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.

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 personal information wherever possible. If you disclose identifiable information for purposes other than a patient's direct care or local clinical audit 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 (see paragraphs 87–94).

   b. The patient has given explicit consent (see paragraph 95).

   c. The disclosure is approved through a statutory process which 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 105–112).

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

1
About this guidance

2 The use of information about patients is essential to the education and training of medical students, doctors in training and other healthcare students and trainees. This explanatory guidance sets out how the general principles in our guidance Confidentiality apply in the particular context of education and training.

General principles

3 For most education and training uses, anonymised information will be sufficient and must be used whenever practicable. If it is necessary to use identifiable information about a patient, or it is not practicable to anonymise information, you should usually ask for the patient’s explicit consent before disclosing it to anyone who is not part of the team that is providing or supporting the patient’s direct care. You should make sure that the patient is under no pressure to consent. In particular, you should avoid any impression that their care depends on giving consent.2

Teaching and training of medical students, doctors in training and other healthcare students and trainees

4 Most patients understand and accept that the education and training of medical students, doctors in training and other healthcare students and trainees relies on them having access to information about patients. If doctors in training or medical or healthcare students are part of the team providing or supporting a patient’s direct care,3 they can have access to the patient’s personal information, just as other team members do, unless the patient objects.4

5 If the doctor or student is not providing or supporting the patient’s care, anonymised information should be used for education and training purposes whenever practicable. This may not be achievable, for example, on ward rounds, but it will then usually be possible to seek the patient’s explicit consent to disclosure.

6 In some cases it might be necessary to disclose personal information, or not practicable to anonymise it, or to ask for a patient’s consent. In such cases you may disclose relevant personal information to medical students, doctors in training and other healthcare students and trainees, as long as you are satisfied that information has been made readily available to the patient about the disclosure and of their right
to object, and they have not objected. You must also be satisfied that they understand that the information is given in confidence, which they must respect.

**Patients who lack capacity**

7 You should not disclose personal information for education and training purposes about patients who lack capacity if you can use information about other patients instead.

8 If you wish to disclose personal information about a patient who currently lacks capacity (for example, because they are acutely unwell), but who is likely to regain capacity, you should wait and ask for their consent later if you can.

9 If you are asked, or want, to disclose information about a patient who lacks capacity, you should seek the views of anyone the patient asks you to consult, or who has legal authority to make decisions on their behalf, or who has a close personal relationship with the patient. They may be able to give you an indication of the patient’s previously expressed preferences, views and beliefs.

10 In the absence of any indication about the preferences of a patient who lacks capacity, you should not publish information from which they can be identified. In exceptional cases, however, you may disclose relevant personal information to medical students, doctors in training and other healthcare students and trainees if it is necessary for their education and training. You must be satisfied there is no reasonably practicable alternative to using personal information, and you should have no reason to believe that it is contrary to the interests of the patient to do so.

**Disclosing information to secondary school and college students**

11 Doctors are sometimes asked to provide work experience for secondary school or further education college students, which may include allowing them to be present during consultations with patients.

12 You should ask for the patient’s explicit consent to a student observing their care. You should also satisfy yourself that the student’s presence does not adversely affect the patient’s care, for example by inhibiting frank discussion.
13 You should satisfy yourself that the student understands the importance of respecting confidentiality and that their school or college takes seriously its responsibilities for its students’ conduct.  

Training records and case studies

14 You must anonymise patient information in training records and case studies as far as it is possible to do so. The anonymisation code of practice published by the Information Commissioner’s Office 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. Simply removing the patient’s name, age, address or other personal identifiers is unlikely to be enough to anonymise information to this standard.

15 If it is difficult to anonymise information about patients while retaining enough detail to make a training record useful, or if it is necessary to include identifiers (such as the patient’s hospital number) to allow the record to be audited, you should ask for the patient’s consent to use their information if you can. If is not practicable to seek the patient’s consent, you may use potentially identifiable information in a training record as long as you are satisfied that the record will be kept securely and will be managed in accordance with other data protection requirements. You must still remove as many identifiers as you can.

16 If the information is likely to be more widely accessible (for example, in discussion at a seminar or conference, or published in a journal), and you consider that the patient could be identified, you should usually use the information only when you have the patient’s explicit consent.

17 When asking for the patient’s consent, you must give the patient enough information about the nature and purpose of the disclosure to enable them to make an informed decision. This should include a description of the information to be disclosed and an indication of who will have access to it and how it will be used.

18 You may disclose information only for the purposes for which the patient has given consent, and you must remove as many identifiers as you can. You must respect a patient’s refusal to consent to the publication of their identifiable information.
If for any reason you cannot get a patient’s consent – for example, because the information you want to disclose is so old that efforts to trace the patient have been or are likely to be unsuccessful – you will need to consider whether disclosing potentially identifiable information can be justified in the public interest. You should seek advice from 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 disclosing personal information without consent.

Endnotes

1 All paragraph numbers in this section refer to our guidance Confidentiality. You can find all of our guidance online at www.gmc-uk.org/guidance.

2 See our guidance Consent: patients and doctors making decisions together, which states that you must give patients the information they want or need about the extent to which students may be involved in their care, and of their right to refuse to take part in teaching.

3 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.

4 See paragraphs 28–29 of Confidentiality for advice on implied consent.

5 Welfare attorneys, court-appointed guardians and court-appointed deputies have legal authority to make some decisions on a patient’s behalf. For disclosure in the public interest, you will be seeking their views about the patient’s preferences, rather than their consent to disclose.


8 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).

9 See paragraphs 106–112 of Confidentiality for guidance on assessing whether a disclosure would be justified in the public interest.
Responding to criticism in the media

1 In our guidance Confidentiality we say:

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

About this guidance

2 Doctors are sometimes criticised in the print or broadcast media or on social media by their patients or by someone who is close to, or who represents, a patient. The criticism can include inaccurate or misleading details of the doctor’s diagnosis, treatment or behaviour. Although this can be frustrating or distressing, it does not relieve you of your duty to respect your patient’s confidentiality. This explanatory guidance sets out how the general principles in our guidance Confidentiality apply when doctors are considering how to respond to criticism in the media.

Responding to criticism

3 Disclosures of patient information without consent can undermine the public’s trust in the profession as well as your patient’s trust in you. Disputes between patients and doctors conducted in public can also prolong or intensify conflict and may undermine
public confidence in the profession, even if they do not involve the disclosure of personal information without consent.

4 You must not put information you have learned in confidence about a patient in the public domain without that patient’s explicit consent. You should usually limit your public response to an explanation of your legal and professional duty of confidentiality.

5 However, from time to time, media reports or social media discussions might cause patients to be concerned about your practice, or that of a health service you are associated with. In such cases it may be appropriate to give general information about your normal practice. You must be careful not to reveal personal information about a patient, or to give an account of their care, without their consent. If you deny allegations that appear in public media, you must be careful not to reveal, directly or by omission or inference, any more personal information about the patient than a simple denial demands.

6 You should seek advice from your professional or defence body, or from a solicitor, on how to respond to criticism in the media and, if appropriate, any legal redress available to you.

---

1 See also our guidance *Doctors’ use of social media*. You can find all of our guidance online at www.gmcuk.org/guidance.

2 In this guidance, ‘patient’ refers to both current and former patients.
Explanatory statement - Reporting gunshot and knife wounds
Reporting gunshot and knife wounds

1. In our Confidentiality guidance we say:

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

   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.

   62 You should ask for a patient’s consent to disclose information for the protection of others unless it is not safe or practicable to do so,¹ or the information is required by law. You should consider any reasons given for refusal.

   64 If it is not practicable 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 public and the patient’s interest in keeping the information confidential.

   68 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. You should inform the patient before disclosing the information, if it is practicable and safe to do so, even if you intend to disclose without their consent.
**About this guidance**

2. This explanatory guidance sets out how the principles in our guidance *Confidentiality* apply when a patient presents with a gunshot wound or a knife wound that is not self-inflicted.

3. The principles in *Confidentiality* and this guidance apply to all violent injuries, but gunshot and knife wounds raise issues that warrant special consideration, given the potential immediacy of risk to others.

**Reporting gunshot and knife wounds**

4. The police are responsible for assessing the risk posed by a member of the public who is armed with, and has used, a gun or knife in a violent attack. They need to consider:

   - the risk of a further attack on the patient
   - the risk to staff, patients and visitors in the emergency department or hospital
   - the risk of another attack near to, or at, the site of the original incident.

The police also need statistical information about the number of gunshot and knife injuries, and when and where they occur, to inform their own and their crime reduction partners’ operational and strategic priorities.

5. For these reasons, the police should usually be informed whenever a person presents with a gunshot wound. Even accidental shootings involving lawfully held guns raise serious issues for the police about, for example, firearms licensing.\(^2\) The police should also usually be informed when a person presents with a wound from an attack with a knife, blade or other sharp instrument.

6. The police should not usually be informed if a knife or blade injury appears to be accidental, or a result of self-harm. There may also be other circumstances in which you consider that contacting the police is not proportionate. For example this might be
the case if you consider that no one other than the patient is at risk of harm, and that contacting the police might cause the patient harm, distress, or may damage their trust in you or in doctors generally.

7. If you are in doubt about the cause of an injury, you should if possible consult an experienced colleague.

Making the report
8. If you are responsible for the patient, you should make sure that the police are contacted where appropriate, but you can delegate this task to another member of staff.

9. Personal information, such as the patient’s name and address, should not usually be disclosed in the initial contact with the police. The police will respond even if the patient’s identity is not disclosed.

Make the care of the patient your first concern
10. When the police arrive, you should not allow them access to the patient if this will delay or hamper treatment or compromise the patient’s recovery.

11. If the patient’s treatment and condition allow them to speak to the police, you or another member of the healthcare team should ask the patient whether they are willing to do so. If they are not, you, the rest of the healthcare team, and the police must abide by the patient’s decision.

Disclosing personal information without consent
12. If it is probable that a crime has been committed, the police will ask for more information. If practicable, you should ask for the patient’s consent before disclosing personal information unless, for example, doing so:

- may put you or others at risk of serious harm
- would be likely to undermine the purpose of the disclosure, by prejudicing the prevention, detection or prosecution of a crime.
13. If the patient refuses consent or cannot give it (e.g., because they are unconscious), you can still disclose information if it is required by law or if you believe disclosure is justified in the public interest.

14. Disclosures in the public interest may be justified when:

- failure to disclose information may put someone other than the patient at risk of death or serious harm (you should not usually disclose information against the wishes of an adult patient who has capacity if they are the only person at risk of harm³)

- disclosure is likely to help in the prevention, detection or prosecution of a serious crime.

15. If there is any doubt about whether disclosure without consent is justified, the decision should be made by, or with the agreement of, the consultant in charge or the healthcare organisation’s Caldicott or data guardian.

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

17. Unless it is not practicable or safe to do so, you should tell the patient about any disclosures that have been made as soon as possible after the disclosure.

18. If there is no immediate reason for disclosing personal information in the public interest, no further information should be given to the police. The police may seek an order from a judge or a warrant for the disclosure of confidential information.⁴

**Children and young people**

19. Any child or young person under 18 years arriving with a gunshot wound or a wound from an attack with a knife, blade or other sharp instrument is likely to raise child
protection concerns. Knife or blade injuries from domestic or occupational accidents, or from possible self-harm, might also raise serious concerns about the safety of children and young people.

20. You should follow the advice in *Protecting children and young people: the responsibilities of all doctors* whenever you are concerned that a child or young person has experienced, or is at risk of, serious harm.

---

**Endnotes**

1. We give examples of when it might not be practicable to seek consent in paragraph 14 of *Confidentiality*. You can find all of our guidance online at [www.gmc-uk.org/guidance](http://www.gmc-uk.org/guidance).

2. The police are responsible for deciding whether an individual is fit to hold a shot gun or firearms licence. Disclosure of information to the police may be justified in the public interest to inform this decision if failure to disclose the information may expose others to a risk of death or serious harm.

3. See *Confidentiality*, paragraphs 57–59, for further guidance.

4. See schedule 1 of the Police and Criminal Evidence Act 1984, schedule 1 of the *Police and Criminal Evidence (Northern Ireland) Order 1989* and section 135 of the *Criminal Procedure (Scotland) Act 1995*. The police can also use powers to seize evidence, such as clothing, that may help in detecting or prosecuting crime.
Plans for launch of the guidance in January 2017

1. The guidance will be launched in January 2017 and will come into effect in April 2017. This is usual practice for our professional guidance. It allows time for key users - not just individual doctors, but also organisations such as the defence bodies and professional associations - to become familiar with the guidance and to update their own reference materials where necessary.

2. This gap between publication and the guidance coming into force means that the current confidentiality guidance and associated materials will remain in effect until April 2017. Our communication and engagement activity will make these timings clear to doctors and others, to help prevent confusion about which guidance to follow.

3. In January we will publish the pdf of our new guidance on our ‘News and consultations’ and ‘Confidentiality review’ pages. The guidance will be watermarked to make it clear that it is not yet in effect. Hard copies will be available for our external relationship teams, including the devolved offices, contact centre and Regional Liaison Service, to distribute on request.

4. The new guidance will not appear on our guidance pages and will not be added to the GMC app or published in e-book format until it comes into effect in April. At this point a suite of products will be launched to support doctors in applying the guidance in practice.

Implementation of the guidance from April 2017

5. Confidentiality is a highly complex area of law and practice, and our guidance is necessarily long, nuanced and detailed in places. We do not expect most doctors to read it from end to end. We therefore need to make sure that the guidance is designed in such a way that doctors can quickly and easily find the advice they need. We also want to publish a range of materials that will support doctors in applying the guidance in practice.
6 The rest of this annex summarises current thinking on how we can ensure that the guidance and supporting materials are accessible, useful and relevant to very busy doctors who may need to refer to it in a wide variety of situations and contexts.

**The guidance - one source, multiple formats**

7 The classic format of the guidance – as a downloadable or printed booklet – is an important one for some of our key audiences. For example we know that advisors in the BMA and defence bodies keep heavily annotated versions of our booklets close by and use them to advise doctors. The booklet is also a good format for formal scrutiny, for example by the courts.

8 But we also need to make sure the guidance is accessible and useful for working doctors. The digital strategy is giving us new ways to make the guidance interactive and searchable (and potentially to enable some tailoring of content to customer needs and interests). GMC guidance has been readable on mobile devices and online for some time, but last year we launched an e-book version of eight guidance booklets which can be downloaded to Kindle devices, or to tablets and mobile phones. We recently launched the Standards app – My GMP – which brings all of our professional guidance together in a format that can be easily accessed at the point of need (including offline) and can always be close to hand.

9 We have written the guidance with these electronic formats in mind. While the guidance can be read from end to end, it is also structured in discrete ‘chunks’, with succinct headings, which can be accessed from an electronic contents page. Given the complexity of the material it is not possible for all sections to be read in isolation, so we will use hyperlinks to help the reader navigate the guidance. We will also use the flowchart as a navigation tool in pdf and html versions (and possibly in e-books and later phases of the app).

**Short guides**

10 We are also considering ways of abbreviating the guidance in stand-alone documents for publication in April 2017. Such ‘short guides’ are however notoriously difficult to produce without oversimplifying the material to the point of it being unhelpful and/or incompatible with the complex and nuanced legal framework. We also risk confusing doctors about what guidance actually binds them, as distinct from supporting materials intended to assist. Defence bodies in particular argue that there should be clarity about what does, and doesn’t, have the status of ‘GMC guidance’, given its potential relevance to fitness to practise investigations. We also risk having inadvertently incompatible advice in different places.

11 We are therefore exploring options that take account of these risks. One possible model for doctors is to draw together the flowchart and key principles, along with a Q&A section which aims to summarise the advice provided in the guidance, while making clear that it does not replace the guidance. Another approach is to create...
pocket size ‘fold-up’ documents which contain the flowchart and key principles. We produced credit-card size fold-up materials of this kind for the child protection guidance, and they were (and still are) very well received. We will test these formats with our growing user group of working doctors.

12. It is easier to provide short guides for audiences that are not bound by our guidance – such as medical students and patients. We will engage with medical schools and patient organisations and charities to explore the value of creating these additional materials.

a. Communicating the new guidance to medical students will be a priority. We hope to do this in conjunction with the ongoing implementation of our new student professionalism guidance, *Achieving good medical practice*. *Achieving good medical practice* was jointly developed with the Medical Schools Council (MSC), and we have proposed drawing up ‘implementation sessions’ with them, to deliver to medical schools and their students via our Regional Liaison Service. The key messages from the new confidentiality guidance could be integrated in these sessions. We are seeking a meeting with the MSC to discuss this further.

b. In respect of the patient guide, we will consider whether it is possible to produce something which outlines what patients can expect from their doctors and when (and on what basis) their information might be disclosed. In the core guidance, we advise doctors to take steps to ensure that patients are aware of how their information might be used, and such a document might help them in doing so.

**Case studies and other decision aides**

13. Over the past ten years we have developed a wide variety of supporting materials to help to illustrate how the principles in GMC guidance might apply in practice. These include interactive case studies (GMP in Action) and static case studies (published in pdf form on the relevant guidance page), all of which are accessed from the GMC website.

14. We plan to develop a range of new case studies, and expand on some existing ones, to show how the principles in the confidentiality guidance apply across a variety of specialties and settings, illustrating all the various stages of decision making set out in the flowchart. These can be made available online as interactive and static case studies, as RLS modules, or as online training resources (depending how we want to progress this in the context of GMC Services). Our plan is to publish a suite of case studies as resources for the regional and devolved liaison services in April 2017.

15. Longer term, and subject to budgetary approval, we would also like to use the flowchart as an interactive decision tool on our website, linking to the guidance and to illustrative scenarios. We have taken this approach with the raising concerns toolkit and the recent mental capacity decision tool, both of which have been well received.
The underlying logic of the confidentiality guidance lends itself particularly well to
decision tools that help doctors to ask the right questions in the right order, and
responses to the pre-consultation engagement told us that there is a clear appetite
among doctors for interactive tools to help structure decision making

We could also explore the possibility of working with others (such as education
providers) to develop educational materials such e-learning modules. We have done
this before. In 2009/10 we worked with e-learning for health to develop a module on
our guidance *Treatment and care towards the end of life* which forms part of the
overall package of e-learning on end of life care. There is however no shortage of
e-learning on confidentiality and information governance; a short audit found twelve
e-learning packages from organisations such as the BMJ, NHS Scotland, NHS Digital,
NHS Wales, Health Education England and a range of private providers. Further
market analysis would therefore be needed before we commit to this course of action.