Ethics Toolkit

Confidentiality

January 2024
(updated February 2025)

BMA Medical ethics and human rights

bma.org.uk

Contents

About this toolkit

Questions about confidentiality are a significant area of ethical enquiry for the BMA. Our toolkit provides answers to commonly asked questions about when confidential information can be disclosed which reflect the ever-growing list of demands to share information. Its 15 sections cover specific areas of confidentiality such as disclosing information with consent, disclosing information in the public interest and dealing with requests from third parties.

There are separate sections dealing with adults lacking capacity and deceased patients. The toolkit does not deal with children and young people. The BMA has a separate children and young people toolkit which deals with issues of confidentiality relating to this group.

The toolkit does not aim to be definitive guidance on all issues surrounding confidentiality and it points you to useful guidance from other bodies, such as the General Medical Council (GMC), that you should use along with our guidance.

You can use each section alone, although there are some areas of overlap. Section 1 is relevant to all disclosures of confidential information.

This Toolkit is available on the BMA's website. Individual healthcare professionals, Trusts, Health Boards and medical schools may download it and make copies.

The BMA would welcome feedback on the usefulness of the toolkit. If you have any comments, please address them to:

Medical ethics and human rights department
British Medical Association
BMA House
Tavistock Square
London
WC1H 9JP
Email: ethics@bma.org.uk
Website: www.bma.org.uk

1 Introduction to the main principles of confidentiality

The duty of confidence

Confidentiality is essential to the relationship of trust between doctors and patients. The principles of confidentiality apply to all doctors irrespective of their speciality. Patients must be able to expect that information about their health which they give in confidence will be kept confidential unless there is a compelling reason that it should not be.

There is a strong public interest in confidentiality as it encourages individuals to seek medical treatment when they need it and freely share information with the healthcare professionals who are providing that treatment. If patients feel they can share information securely for their own care this also ensures there is reliable health information available for approved medical research and health service planning that advances medical knowledge and improves care for patients. The duty of confidentiality extends beyond a patient's death.

Patients also expect that confidential information will be shared with others involved in delivering their care. See 3 on disclosing information with consent.

When does a duty of confidence arise?

'A duty of confidence arises when confidential information comes to the knowledge of a person…in circumstances where he has notice, or is held to have agreed, that the information is confidential…'
Lord Goff. Campbell v MGN Limited (2004)

What information is confidential?

There are various legal definitions relating to 'confidential information' or 'confidential patient information'. The term 'confidential information' is used throughout this guidance to mean information from which patients can be identified and in respect of which a duty of confidence is owed, including information about deceased patients.

'All identifiable patient data held by a doctor or a hospital must be treated as confidential.'
W,X,Y,Z v. Secretary of State for Health (2015)

Demographic information provided by patients for the purpose of registering for, or receiving, healthcare as well as clinical information, is confidential. Even where demographic information is held separately from clinical information, such as a list of patients' names and addresses, it is equally subject to the duty of confidence.

1

Confidential information can be held in written, digital, visual, or audio form or simply information held in the memory of healthcare professionals. It covers (non-exhaustively):

- NHS Number, or Community Health Index (CHI) number, and names and addresses or other demographic information used to identify patients;
- any clinical information about an individual's diagnosis or treatment;
- a picture, photograph, video, audiotape, scans, ECHGs or other images of the patient or their tests;
- who the patient's doctor is and what clinics the patient attends and when; and
- anything else that may be used to identify a patient directly or indirectly.

When can confidential information be disclosed?

The duty to maintain confidentiality can present healthcare professionals with an ethical or legal dilemma, commonly when a third party requests information about the patient or their treatment. The duty of confidentiality is not absolute and confidential information can be disclosed when one of the following circumstances applies:

- the patient has capacity to consent and consents to the disclosure. This can be either:
  - implied consent for an individual's direct care; or
  - explicit consent (see section 3);
- the law requires disclosure (see section 6);
- the duty of confidentiality has been set aside under section 251 of the NHS Act 2006 (see section 10); or
- where there is an overriding public interest, that is, where disclosure is essential to prevent serious harm to the individual or a third party or to prevent or detect a serious crime in accordance with GMC guidance (see section 7).

Making a disclosure

When making a disclosure of confidential information for purposes other than a patient's direct care, healthcare professionals must:

- ensure that one of the above circumstances applies;
- disclose only the minimum relevant information necessary;
- ensure the disclosure is to the appropriate authority;
- document the disclosure and the reason for it in the medical record;
- be prepared to justify their decisions to disclose (or not to disclose);
- consider and satisfy the Caldicott Principles; and
- seek advice from the Caldicott Guardian if there is uncertainty (trainees should refer to a senior consultant or GP partner).

2

Confidentiality: a legal and ethical overview

The legal framework which applies to confidential information combines common law and statutes, for example the General Data Protection Regulation (GDPR) and the Human Rights Act (HRA) 1998. The legal framework is supplemented by ethical and professional guidance from regulatory bodies and obligations under contracts of employment. When considering questions about confidentiality, healthcare professionals must look at the overall effect of the law, ethical guidance and their contractual obligations, not just each aspect in isolation.

Disclosure of, and access to, confidential information is governed by the below, all of which are reflected throughout this guidance.

The Common Law

The common law is based on previous decisions about the law made in court by judges – sometimes referred to as 'judge-made law'. Under the common law duty of confidentiality, if information is received in confidence, including where it is reasonably expected that a duty of confidence applies, that information cannot normally be disclosed without patient consent unless it is required by law (section 6), when the duty of confidentiality is set aside via section 251 of the NHS Act 2006 (section 10), or where there is an overriding public interest (section 7).

Human Rights Act 1998

A right to 'respect for private and family life' is guaranteed in article 8 of the HRA. This right is not absolute, and may be set aside by the state where the law permits and 'where 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'. The effect is similar to that of the common law: privacy is an important right which must be respected, but interference with it can be justified in certain circumstances.

Data Protection Act 2018 and the UK General Data Protection Regulation

The Data Protection Act 2018 (DPA) is the primary piece of data protection legislation in the UK and incorporates the GDPR into UK law. The DPA sits alongside, and supplements, the UK GDPR. It applies to all personal data relating to living individuals, including confidential information.

The DPA regulates the processing of personal data about living individuals including disclosing, holding, or using information. It applies to paper records, digital information, and images of individuals. A fundamental requirement of UK GDPR is transparency. As part of satisfying transparency requirements, healthcare organisations must use privacy notices which are easy for patients to find and which explain how confidential information is used and shared.

The BMA has separate guidance on UK GDPR which outlines how to handle special category health data (see key resources). If you are a GP data controller under UK GDPR it is particularly important that you familiarise yourself with this guidance.

2

Access to Health Records Act 1990

The UK GDPR and DPA do not cover the records of deceased patients. Rights of access to deceased patients' health records are contained within the Access to Health Records Act 1990 and Access to Health Records (Northern Ireland) Order 1993. Personal representatives (executors or administrators of the estate of a deceased person) have the right to access the deceased's health records. A person who may have a claim arising from the death of the deceased may also access the deceased's health records, but their access is limited to information which is directly relevant to the claim.

National Health Service Act 2006

In England and Wales, regulations under section 251 of the NHS Act 2006 permit certain disclosures to occur without a breach of the common law duty of confidentiality.

The Health Service (Control of Patient Information) Regulations 2002 can provide statutory support to enable health service management and medical research when it is not practical to obtain consent and anonymised information cannot be used. Disclosures under these regulations are commonly referred to as having 'section 251 support' (see section 10).

Computer Misuse Act 1990

It is an offence under the Computer Misuse Act to gain unauthorised access to computer material. This includes using another person's ID or login details and password without authority in order to do so, or to alter or delete data.

Caldicott Principles

There are eight good practice Caldicott Principles which apply to all confidential data collected for the provision of health and social care services. Organisations providing publicly funded health or care services should appoint a Caldicott Guardian whose role is to help their organisation to uphold the Caldicott Principles.

Contract of employment

Confidentiality of patient information is a requirement of NHS employment contracts and the employment contracts of independent providers of NHS services. Staff employed by the NHS may face disciplinary action by their employer if they breach confidentiality.

Professional and ethical standards

All healthcare professionals must maintain the standards of confidentiality laid down by their professional body, such as the General Medical Council (GMC) and Nursing and Midwifery Council (NMC), or risk complaint for professional misconduct which may result in a reprimand or removal from the register.

Key resources

BMA – GPs as data controllers under GDPR
BMA – Access to health records
UK Caldicott Guardian Council – A manual for Caldicott Guardians

3

Disclosing information with consent

Consent to disclosure may be implied or explicit. In either case, consent should be informed and freely given.

When can consent be implied?

Healthcare professionals rely on implied consent when sharing information for the direct care of an individual patient (unless the patient has indicated an objection). This well-established practice is based on the understanding that patients will expect that those providing them with direct care will have access to information needed to support the safe and effective provision of their care.

What is direct care?

Direct care activities are those that directly contribute to the diagnosis, care (including preventative care), and treatment of an individual patient.

Those providing direct care are considered to have a 'legitimate relationship' with the individual patient. This includes non-healthcare professionals, such as social workers, and clerical staff, when they are involved with the provision of direct care to the patient. Information sharing amongst those with a legitimate relationship is acceptable to the extent that health and care professionals only share relevant information on a 'need to know' basis.

Local clinical audits are an integral part of direct care. They can therefore be conducted with implied consent provided the audit is carried out by a clinician with a legitimate relationship with the patient (and where it is not possible to use anonymised information).

When is a legitimate relationship created?

A legitimate relationship is created with a registered and regulated health or social care professional when any or all of the following criteria are met:

- the individual presents themselves to the professional to receive care;
- the individual agrees to a referral from one care professional to another;
- the individual is invited by a professional to take part in a screening or immunisation programme for which they are eligible and they accept;
- the individual presents to a health or social care professional in an emergency situation where consent is not possible;
- the relationship is part of a legal duty, for example, contact tracing in public health; and/or
- the individual is told of a proposed communication and does not object.

Read more in the Caldicott Review (see key resources).

The question of when a legitimate relationship is created is particularly important in the context of integrated care models or multi-agency working. The basic rule is that if a legitimate relationship has not been created, consent for records to be accessible across organisational boundaries cannot be implied. There may be some exceptions to this for local out of hours service arrangements, including out of hours pharmacies, when certain information such as current medication, allergies, and key medical history can be shared.

3

'No surprises'

When considering sharing information for direct care reasons a useful rule of thumb to apply is that patients should not be surprised to find out who has been given access to their information. To ensure there are 'no surprises', and for implied consent to be valid, it is important that patients are informed about how their information is shared and that they can object. It is important that when sharing information with implied consent healthcare professionals do not go beyond the purposes which a patient has been informed about and might reasonably expect. One way to help ensure 'no surprises' is via the use of privacy notices which explain how information is used and shared and which are an essential requirement of the UK GDPR.

Importance of sharing for direct care

'The duty to share information for individual care is as important as the duty to protect patient confidentiality.' Principle 7, The Caldicott Principles.

It can be frustrating for patients to repeat the same information to multiple healthcare professionals. In England, the Health and Social Care (Safety and Quality) Act 2015 imposes a statutory duty on healthcare providers and commissioners to share information for the provision of health or care to an individual. This duty does not override the obligations of the common law duty of confidentiality. For the provision of direct care this means the patient's implied consent is required as described above.

Can patients object to sharing information for direct care?

Yes. The objection of an adult patient with capacity to information sharing for direct care purposes should be respected (unless, in rare circumstances, there is a public interest justification for the disclosure, see section 7). Any refusal of disclosure must be documented in the medical record.

The potential consequences of the patient's refusal to share with others providing their care should be explained to them and options for compromise explored. Ultimately, it may not be possible to refer or treat the patient if it would be unsafe or harmful to do so without disclosing information.

When is explicit consent needed?

If the sharing is not among the health and care team who are providing (or have provided) direct care to the patient, explicit consent is required unless there is another lawful justification in place (see section 1). Explicit consent is achieved when a patient actively provides consent, either orally or in writing. A common example of when explicit consent is required is for disclosures to local councils providing housing or benefits services.

3

HIV and Sexually Transmitted Infections (STIs)

Information disclosed by a patient to a dedicated sexual health service should not be shared with other healthcare professionals, including the patient's GP, without the patient's explicit consent.

Other health services which provide STI and HIV treatment must inform patients about how their information will be shared, including how information will be accessible within a shared care record. If HIV/STI information is to be shared on the basis of implied consent, healthcare professionals must be confident that the patient has a reasonable expectation that this will happen. A patient's choice not to share information with other health and care professionals involved in their care must be respected, unless the disclosure can be justified in the public interest (see section 7).

Key resources

Caldicott F – To share or not to share? The information governance review
GMC – Confidentiality: good practice in handling patient information

4

Adults lacking capacity

Healthcare professionals have the same duty of confidentiality to all their patients regardless of age or disability. Patients with mental health problems or learning disabilities must not automatically be regarded as lacking capacity to give or withhold their consent to the disclosure of confidential information.

The BMA has separate guidance on treating adults who lack capacity (see key resources).

In the absence of a health and welfare attorney or other lawful proxy decision maker, healthcare professionals may only disclose information on the basis of the incapacitated patient's best interests or, in Scotland, where it provides a 'benefit' to the patient. Where patients lack mental capacity to consent to disclosure, it is usually reasonable to assume that patients would want people close to them to be given information about their illness, prognosis, and treatment unless there is evidence to the contrary. However, where there is evidence that the patient did not want information shared, this must be respected.

Those close to the patient who lacks capacity have an important role to play in decision making whether they have a formal role as a proxy decision maker, or a more informal role such as helping the healthcare team to assess the patient's best interests. It might, however, be more difficult to carry out these roles without some information being provided about the medical condition of the patient.

Proxy decision makers

Legally-appointed proxy decision makers have the right to give or withhold consent to treatment and so must be involved in treatment decisions, although where emergency treatment is required this may not always be possible or practicable. Legally-appointed proxy decision makers include welfare attorneys and court-appointed deputies whose authority extends to medical decisions and persons authorised under an intervention order or welfare guardians with powers relating to the medical treatment in question. It follows that they have rights of access to sufficient information to enable them properly to make the decisions they are charged with.

Independent mental capacity advocates (IMCAs) – England and Wales

Where a patient in England and Wales lacks capacity and has no relatives or friends who can be consulted - or whom it is appropriate to consult – the MCA requires an IMCA to be appointed and consulted about all decisions about 'serious medical treatment', or place of residence. The healthcare team must provide the IMCA with all the relevant information including the risks, benefits, side effects, likelihood of success and level of anticipated improvement if treatment is to be given, the likely outcome if treatment is withheld, and any alternatives that might be considered.

While it will therefore be necessary for all lawful proxy decision makers to have information that will enable them to act or make decisions on behalf of the patient, it does not mean that they will always need to have access to all the patient's records. Only information relevant to the issue in question should be disclosed.

4

Relatives, carers, and friends

If a patient lacks capacity, healthcare professionals may need to share information with relatives, friends, or carers to identify the care or treatment that is in the patient's overall best interests, or that will benefit the patient. Where a patient is seriously ill and lacks capacity, it would be unreasonable always to refuse to provide any information to those close to the patient on the basis that they have not given explicit consent. This does not however mean that all information should be routinely shared and, where the information is particularly sensitive, a judgement will be needed about how much information the patient is likely to want to be shared and with whom. Where there is evidence that the patient did not want information shared, this must be respected.

Disclosures to protect adults who lack capacity

There are certain legal requirements to disclose information about an adult who may be at risk of harm (see section 6).

In the absence of a legal requirement, where adults lack the capacity to make a decision about whether or not to disclose information relating to harm or abuse, decisions need to be made on their behalf. Decisions can be made by a legally appointed proxy or (if one is not available) relevant healthcare professionals can make a decision based upon an assessment of the individual's best interests or of what would be likely to benefit them.

When considering a disclosure of information, any assessment of best interests or benefit will ordinarily involve discussion with those close to the individual. In relation to domestic abuse, however, care has to be taken to ensure that anyone consulted who is close to the individual is in fact acting in the person's interests.

Healthcare professionals must disclose information to the appropriate authority where there is a belief that an adult lacking capacity is at risk of abuse or other serious harm, unless it is not in the overall best interests of the patient to do so.

Where attorneys appear to be making decisions that are clearly not in the best interests of the individual, and the problems cannot be resolved locally, the matter should be referred in England and Wales to the Court of Protection. In Scotland, decisions about medical treatment are open to appeal to the sheriff and then, by leave of the sheriff, to the Court of Session. Further information is available from the Scottish Mental Welfare Commission.

Disclosures to the Office of the Public Guardian (OPG) (England and Wales)

In England and Wales, the Office of the Public Guardian (OPG), or a Court of Protection visitor acting on the instructions of the OPG, may ask a healthcare professional to see a patient's records while it is investigating the actions of a deputy or attorney. For example, the OPG may want to establish the mental capacity of a patient at a particular time. If healthcare professionals can release this information promptly, it can help ensure these investigations are completed as quickly as possible. If the request from the OPG concerns a patient who has capacity however, explicit consent for disclosure from the patient must be sought.

Key resources

BMA – Mental Capacity Act toolkit
BMA – Adults with incapacity Scotland toolkit
BMA – Mental capacity in Northern Ireland toolkit

5

Deceased patients

Are deceased patients owed a duty of confidentiality?

Yes. The obligation to respect a patient's confidentiality extends beyond death. However, this duty needs to be balanced with other considerations, such as the interests of justice and of people close to the deceased person. There may be some circumstances where it is obvious that there may be some sensitivity about information in health records. In these limited circumstances healthcare professionals may wish to consider speaking to their patients about the possibility of disclosure after death with a view to soliciting their views about disclosure.

Are there any rights of access to a deceased patient's records?

Statutory rights of access are contained within the Access to Health Records Act 1990 (AHRA) and the corresponding legislation in Northern Ireland, the Access to Health Records (Northern Ireland) Order 1993.

There are two distinct groups who have rights of access to information within the deceased's record:

– personal representatives; and
– anyone who may have a claim arising out of a patient's death.

It is necessary to consider access requests by these two groups separately. A personal representative (the executor or administrator for the estate of a deceased person) does not need to have a claim arising out of the death to access the deceased's medical record. This right of access extends to all information within the record with limited exceptions (see below). Personal representatives do not need to provide a reason for seeking access to the record, although the record-holder must be able to establish that the requestor is indeed the personal representative.

Those who do not have the status of personal representative but may have a claim arising out of the death of the patient, for example an insurance claim, have a right of access only to information which is directly relevant to the claim.

The BMA encourages doctors to adopt an ethical approach to handling requests from personal representatives so that a balance can be achieved between the duty of confidentiality to the deceased and compliance with the legal duty to provide access. In order to maintain confidentiality as far as possible, the BMA advises that when personal representatives request access, it is appropriate to enquire why access is required and whether the request can be satisfied by providing access only to information which is relevant for the purpose. Ultimately, if the personal representative chooses not to provide a reason for access and insists on access to the full record, doctors must comply with these requests to comply with the law.

Medical examiners

Medical examiners have a statutory right of access to the records of deceased patients under section 3 of the AHRA.

5

When should information not be disclosed?

Information requested by personal representatives and others with a claim arising out of the death should not be disclosed if:

- it identifies a third party without that person's consent unless that person is a healthcare professional who has cared for the patient;
- the patient provided it in the expectation that it would not be disclosed to the particular individual making the application;
- it is the result of a particular examination or investigation which the patient consented to in the expectation that it would not subsequently be disclosed;
- in the opinion of the relevant healthcare professional, it is likely to cause mental or physical harm to an individual; or
- the record includes a note, made at the patient's request, that the patient did not wish access to be given.

Who is responsible for providing access?

Medical records of the deceased might be sent to relevant local archive bodies, however, where a provider, such as a GP practice, still holds the record it is obliged to respond to requests under the AHRA (or corresponding legislation in Northern Ireland). Our guidance on access to health records provides more detail on who must give access under the legislation (see key resources).

Are there any other circumstances when information about a deceased patient must be disclosed?

Yes. Separate to the access to health records legislation, information about a deceased patient must be disclosed:

- to assist a coroner or procurator fiscal investigation;
- for accurate completion of death certificates;
- to meet a statutory duty of candour; or
- when the law requires disclosure.

Are relatives entitled to information about the deceased's last illness?

Whilst there is no legal entitlement other than the limited circumstances covered under access to health records legislation, healthcare professionals have always had discretion to disclose information to a deceased person's relatives or others when there is a clear justification. A common example is when the family requests details of the final illness because of an anxiety that the patient might have been misdiagnosed or there might have been negligence. Disclosure in such cases is likely to be what the deceased person would have wanted and may also be in the interests of justice. Refusal to disclose in the absence of evidence that this was the deceased patient's known wish exacerbates suspicion and can result in unnecessary litigation. In other cases, the balance of benefit to be gained by disclosure to the family, for example, of a hereditary or infectious condition, may outweigh the obligation of confidentiality to the deceased.

Key resources

BMA – Access to health records
GMC – Confidentiality: good practice in handling patient information

6

Disclosures required by law

Certain statutes and the courts can require healthcare professionals to disclose confidential information, regardless of patient consent. The statutory requirements which healthcare professionals are most likely to encounter are summarised below.

Healthcare professionals must be aware of their obligations to disclose in these circumstances as well as to ensure that they do not disclose more information than is necessary.

Where healthcare professionals have concerns about a disclosure which is legally required, advice can be sought from the Caldicott Guardian or the National Data Guardian.

What statutory requirements to disclose are healthcare professionals most likely to encounter?

Management of health and care services

– *Health and Social Care Act 2012* (England only)
NHS England has powers under the Health and Social Care Act to require confidential information from healthcare providers in certain circumstances. This will usually be in response to directions from the Secretary of State for Health and Social Care or NHS England.

Public health

– *Public Health (Control of Disease) Act 1984 / Health Protection (Notifications) Regulations 2010* (England only)
– *Public Health (Northern Ireland) Act 1967*
– *Public Health etc (Scotland) Act 2008*
– *Health Protection (Notification) (Wales) Regulations 2010*

Healthcare professionals have a statutory duty to report certain notifiable diseases, including infectious diseases and food poisoning, to the appropriate body.

Adults at risk of harm

– *Care Act 2014* (England only)
– *Adult Support and Protection (Scotland) Act 2007*
– *Social Services and Well-being (Wales) Act 2014*

When requested, healthcare professionals are required to disclose relevant information to adult safeguarding boards or local authorities in relation to enquiries about adults considered to be at risk of, or to have suffered from, abuse or neglect. The requirement to disclose under this legislation applies regardless of whether the adult lacks the capacity to make the decision.

Counter-fraud

– *National Health Service Act 2006 and the National Health Service (Wales) Act 2006*
The NHS Counter Fraud Authority has powers to require the production of documents to prevent, detect, and prosecute fraud in the NHS.

– *Local Audit and Accountability Act 2014* (England only)
Confidential information can be required by the government for fraud-prevention data-matching exercises.

6

Female genital mutilation (FGM)

– *Female Genital Mutilation Act 2003* (as amended by the *Serious Crime Act 2015*) (England, Wales, and Northern Ireland)
In addition to general safeguarding obligations and duties to report in the UK, in England and Wales there is a statutory duty to notify the police when it is identified that an under 18-year-old has had FGM. For more on this issue, see our guidance on children and young people under 16, and guidance on 16 and 17-year-olds (in key resources).

There is no specific statutory duty to report in Northern Ireland, however, the Criminal Law Act would apply – see below.

Regulation of healthcare services

– *Health and Social Care Act 2008 (England and Wales)*
– *Public Services Reform (Scotland) Act 2010*
– *Health and Personal Social Services (Quality, Improvement and Regulation) (Northern Ireland) Order 2003*

Regulatory bodies have powers to access confidential information when it is necessary to perform their regulatory functions.

In Northern Ireland, there are some restrictions on the disclosure of confidential information which mean that identifiable information can be disclosed only in cases of serious risk to individuals.

Investigations by regulatory bodies

– *Medical Act 1983*
The General Medical Council has powers under section 35A of the Medical Act 1983 (as amended) to require disclosure of information relevant to the discharge of fitness to practise functions. The Nursing and Midwifery Council has similar powers.

Northern Ireland: Criminal offences

– *Criminal Law Act (Northern Ireland) 1967*
There is a duty on all citizens to report to the police information they may have about the commission of a relevant offence (in other words, one with a maximum sentence of 5 years or more). This includes a duty to report sexual activity where an over 18-year-old has sex with a young person under 16.

The duty does not arise where a person has a 'reasonable excuse' not to disclose the information. 'Medical confidentiality' is not, in and of itself, understood to be a 'reasonable excuse'.

6

Other legal requirements to disclose

Healthcare professionals may also encounter the below statutory requirements to disclose.

- *Abortion Regulations 1991 (England and Wales) (and amendments); Abortion (Scotland) Regulations 1991; and Abortion (Northern Ireland) (No.2) Regulations 2020;*
  A doctor carrying out a termination of pregnancy must notify the Chief Medical Officer giving a reference number and the date of birth or age and postcode of the person concerned;
- *Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (UK-wide)*
  Employers or those in charge of work premises must report deaths, major injuries, and accidents to the Health and Safety Executive (this duty to report does not extend to doctors who are not employers);
- *Road Traffic Act 1988 (UK-wide)*
  Healthcare professionals must provide to the police on request information which may identify a driver alleged to have committed a traffic offence; and
- *Terrorism Act 2000 (UK-wide)*
  All citizens, including healthcare professionals, must inform police as soon as possible, of any information that may help to prevent an act of terrorism, or help in apprehending or prosecuting a terrorist.

Can patients opt-out of disclosures which are required by law?

No. Patients do not have the right to refuse disclosures which are required by law.

Disclosure to the courts

Courts, including coroner's investigations, have legal powers to require disclosure without patient consent.

Once they have received a court order requiring them to disclose information, healthcare professionals have to comply with it if they think if falls within the scope of what the court needs, however, they should not disclose beyond what has been requested. Refusal to disclose the information can be an offence. If healthcare professionals think information should not be disclosed because, for example, it reveals confidential material about a third party unrelated to the case in hand, they should object to the judge or presiding officer.

Patients must also be given the opportunity to object. If the application is served on a healthcare organisation, rather than an individual patient the patient should be informed of the application so they can make their representations to court if they object.

Key resources

BMA – Children and young people under 16 toolkit
BMA – Treating 16 and 17-year-olds in England, Wales, and Northern Ireland toolkit
BMA – Treating 16 and 17-year-olds in Scotland toolkit
GMC – Confidentiality: good practice in handling patient information

7

Public interest disclosures

When can information be disclosed in the public interest?

Public interest is the general welfare and rights of the public that are to be recognised, protected, and advanced.

According to GMC guidance a disclosure of confidential information because it is in the 'public interest' may be justified if it is essential to:

- prevent, detect, or prosecute serious crime;
- prevent a serious threat to public health or national security; or
- protect individuals or society from serious harm.

In the absence of patient consent, a legal requirement or statutory authorisation, and when the information cannot be anonymised, any decision to disclose confidential information to third parties must be justifiable in the public interest.

Disclosures in the public interest will generally be cases which relate to a single individual's information. Decisions about public interest disclosures must be made on a case-by-case basis. The public interest test cannot be used to justify routine or ongoing disclosures.

Ultimately, the 'public interest' can only be determined by the courts. However, when considering disclosing information in the public interest, healthcare professionals must consider how the benefits of making that disclosure outweighs both the patient's and the public interest in keeping the information confidential. GMC guidance states that when carrying out this balancing exercise doctors must consider (not exhaustive):

- the potential harm or distress to the patient arising from the disclosure;
- the potential harm to trust in doctors generally;
- the potential harm to others if the information is not disclosed; and
- the potential benefits to an individual or society arising from the disclosure of information.

Healthcare professionals must also:

- assess the urgency of the need for disclosure;
- persuade the patient to disclose voluntarily, where appropriate;
- inform the patient before making the disclosure, unless it is unsafe do so or if it would inhibit effective investigation;
- disclose the information promptly to the appropriate body;
- reveal only the minimum information necessary to achieve the objective;
- be assured that the information will be used only for the purpose for which it is disclosed;
- document in the medical record the reasons for disclosing the information without consent (or a decision not to disclose); and
- be able to justify the decision.

7

Healthcare professionals should be aware that they risk criticism or sanctions if they fail to take action to avoid serious harm. Advisory bodies, such as the BMA, cannot tell healthcare professionals whether or not to disclose information in a particular case. They can provide general guidance about the categories of cases in which decisions to disclose may be justifiable. Guidance should be sought from the Caldicott Guardian, senior colleagues, and/or medical defence body where there is any doubt as to whether disclosure should take place in the public interest.

Public interest disclosures will invariably engage one or more of the below considerations.

Is the disclosure necessary to prevent, detect, or prosecute serious crime?

A disclosure in the public interest can be made when it is necessary to prevent, detect, or prosecute serious crime. There is no legal definition as to what constitutes a 'serious' crime. In the BMA's view, serious crime includes murder, manslaughter, rape, treason, kidnapping, violent assault, and abuse of children or similar acts which have a high impact on the victim. Serious harm to the security of the state or to public order and serious fraud will also fall into this category.

A disclosure for serious fraud might be justifiable depending on the facts of the case, for example, serious fraud involving significant NHS resources is likely to harm individuals waiting for treatment. Prescription fraud might be serious, for example if prescriptions for controlled drugs are being forged a disclosure may be justified. In contrast, theft, minor fraud, or damage to property where loss or damage is less substantial is highly unlikely to warrant a breach of confidence.

All healthcare professionals should be aware that even where a crime is 'serious', this fact would not in isolation justify a disclosure on public interest grounds. Healthcare professionals must conduct a balancing exercise involving careful consideration of all relevant factors (see above) in reaching a decision whether the public interest test for disclosure in GMC guidance is met.

Is the disclosure necessary to prevent serious harm?

It is important to distinguish between serious harm to the individual to whom the information relates and serious harm to third parties.

Adults with capacity generally have the right to consent or refuse consent to disclosures of information which expose them (but no one else) to risks of serious harm (see section 8).

In some situations, it may not be possible to seek consent from an adult with capacity, and a disclosure in the public interest is likely to be justifiable to prevent serious harm. An example is when the police are investigating an unexplained disappearance of an individual and have concerns about their safety.

Confidential information can be disclosed without consent to prevent serious harm or death to third parties. Such situations could arise, for example, in domestic violence situations where a child is at risk (see section 8).

Or, if a doctor believes a work place is unsafe and the Health and Safety Executive need identifiable information in order to investigate, a disclosure of confidential information in the public interest may be justifiable.

7

When can information be disclosed to the DVLA or DVA?

Disclosures to the Driver and Vehicle Licensing Authority (DVLA) or Driver and Vehicle Agency (DVA) can be made on public safety grounds. Where a patient has an illness or condition which makes them medically unfit to drive, a prompt disclosure of relevant information should be made to the DVLA or DVA if:

– the patient cannot be persuaded to discontinue driving; or
– the healthcare professional is aware that the patient continues to drive.

Disclosure to the DVLA or DVA is not mandatory, but healthcare professionals must consider whether non-disclosure in relation to a foreseeable and serious threat could leave them open to a possible charge of negligence if grave harm results from the non-disclosure.

Before contacting the DVLA or DVA the doctor should try to inform the patient of their intention to disclose.

Can disclosures be made to prevent the spread of serious communicable diseases?

When a patient has a medical condition that puts others at risk, for example, at risk of infection, healthcare professionals must discuss with the patient how to minimise the risk to others. In the case of serious communicable diseases, healthcare professionals should discuss with the patient how to protect others, for example, in the case of sexually transmitted infections the need for them to inform sexual partners, and the options for safe sex.

Exceptionally, if patients refuse to modify their behaviour or inform others, doctors are advised by the GMC that they may breach confidentiality and inform those at risk of infection, for example a close sexual contact of a patient. Wherever possible, patients should always be told before this step is taken.

There are certain legal requirements, with which public health doctors will be familiar, to disclose information about notifiable diseases to the relevant appropriate bodies for disease control and surveillance purposes (see section 6).

Injuries to colleagues

The use of universal precautions should be enough to protect healthcare workers from infection, thereby making disclosure unnecessary to prevent serious harm. However, there will be occasions where, for example, despite all reasonable precautions a healthcare professional suffers a needlestick or similar injury and the patient is known by the treating doctor to have a blood-borne virus. If the patient has capacity, consent should be sought to disclose information about their infection status.

If the patient cannot be persuaded to consent to disclose their infection status, or if it is not practicable to ask for their consent, the GMC advises that information can be disclosed 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.

The BMA has separate guidance on testing adults who lack capacity in the event of a needlestick injury (see key resources).

7

Can patients object to disclosures in the public interest?

No. If the benefits of the disclosure to an individual or to society outweigh both the public and the patient's interest in keeping the information confidential, the disclosure can occur even in the face of a patient's objection.

The national data opt-out (where patients in England can register to opt-out of their confidential information being used for research and planning purposes) does not apply where there is an overriding public interest in disclosure. (See section 10 for more on the national data opt-out.)

Legal duty to consider a disclosure in the public interest

In rare cases, where a doctor is in a relationship of 'close proximity' with an individual who might benefit from the disclosure of patient information (for example, because knowledge of their genetic risk would enable them to take steps to avoid passing on this condition to their offspring), the doctor could be under a legal duty to balance the duty of confidentiality against the benefits of disclosure in a particular case. (The BMA understands that a relationship of 'close proximity' includes the doctor-patient relationship and, also rare circumstances where a doctor might have a duty of care to a third party.)

If a doctor has carried out the balancing exercise properly, in accordance with professional guidance, and has reasonably concluded that a disclosure should not be made, they will have fulfilled their duty of care. This legal duty reinforces GMC guidance, and the guidance in this section, when doctors face difficult situations whereby the disclosure of a patient's confidential information may benefit others who are at risk. The balancing exercise between benefits and harms must be carried out before a decision to disclose or not to disclose is made.

Key resources

BMA – Needlestick injuries and blood-borne viruses: decisions about testing adults who lack the capacity to consent
GMC – Confidentiality: good practice in handling patient information
GMC – Confidentiality: disclosing information about serious communicable diseases
GMC – Confidentiality: patients' fitness to drive and reporting concerns to the DVLA or DVA

8

Exceptional cases where disclosure without consent is appropriate to protect adults with capacity who are at risk of serious harm

Healthcare professionals can receive requests for information from the police, social services or partnership organisations, such as multi-agency risk assessment conferences (MARACs) in relation to protecting adults who are at risk, or are a victim, of abuse or domestic violence. These requests can present challenging situations where adults with capacity do not want confidential information disclosed, even where this would be the best way to ensure they are protected from harm.

Is consent needed for disclosures to protect adults with capacity from risk of harm?

Whenever doctors seek to disclose confidential information about adults with capacity who are at risk of harm, they should first consider whether they can obtain consent (unless there is a legal requirement to share).

In the BMA's view, adults with capacity have the right to make decisions about how they manage the risks to which they are exposed. Such decisions should ordinarily be respected even where a decision leaves them (but no one else, such as a child) at risk of serious harm. A refusal of disclosure by a patient should not result in the patient being abandoned by services, and continuing care and support should be offered.

In some situations, healthcare professionals may consider disclosing information without consent in the public interest in order to protect adults who have capacity where they have a reasonable belief that the individual will be the victim of serious crime such as violent assault. In these circumstances, healthcare professionals should keep in mind the difficulty of prosecuting a crime where the victim refuses to participate with the criminal justice system, as well as the impact of disclosure on the patient's trust in the profession.

Given the difficulties associated with preventing crime where the victim refuses to cooperate, disclosure of information without consent in these circumstances is likely to be exceptional. Any healthcare professional considering disclosure in these circumstances should take advice from a Caldicott Guardian or appropriate professional, regulatory, or medical defence body and make contemporaneous notes of the decision they make and the reasons behind it.

The advice above relates to situations where only an adult with capacity is at risk. Where others, such as a child or adult lacking capacity are also at risk, a disclosure in the public interest is likely to be justified even in the face of refusal by an adult patient with capacity (see section 7).

Key resources

BMA – Adults at risk and confidentiality
GMC – Confidentiality: good practice in handling patient information

9

Requests from third parties

Doctors receive frequent requests for access to confidential information from third parties for purposes which are unrelated to the provision of healthcare. When third parties ask for confidential information, doctors must have written consent from the patient, or a person properly authorised to act on the patient's behalf, unless there is another lawful basis for the disclosure, such as a disclosure made in the public interest (see section 7).

For disclosures with consent, evidence of consent should be provided by the third party. An electronic copy of a signed form is sufficient, provided that the third party can satisfy the doctor that the form has not been tampered with in any way.

Solicitors

A patient with capacity can authorise a solicitor to make a subject access request (SAR) under UK GDPR on their behalf. As is the case for all SARs, the identity of the person making the request must be verified. Healthcare professionals should treat a request from a patient's legitimately authorised solicitor in the same way as a request from the patient themselves. Solicitors must provide the patient's written consent. The consent must cover the nature and extent of the information to be disclosed (for example, past medical history), and who might have access to it as part of the legal proceedings. Where there is any doubt, healthcare professionals should confirm with the patient before disclosing the information.

Standard consent forms have been issued by the BMA and the Law Society of England and Wales and the Law Society of Northern Ireland (included in the BMA's access to health records guidance - see key resources).

Employers and insurance companies

Insurance companies and employers should use the provisions of the Access to Medical Reports Act 1988 to seek a GP report. Prior to disclosing information to insurers and employers, healthcare professionals must be provided with evidence of the individual's written consent, or authorisation from someone legally able to act on the individual's behalf.

Insurers may sometimes seek to use the SAR provisions of UK GDPR to obtain full medical records. Advice from the Information Commissioner's Office is clear that SARs should not be used to access medical records for insurance purposes. We have separate guidance on this matter (see key resources).

Government departments

Government departments may request information about a patient, for example, to process claims for state benefits. The GMC advises doctors that they may accept an assurance from an officer of a government department or agency that the patient has given written consent to disclosure.

Police

A regular enquiry to the BMA is the right of access to health records by the police. If the police do not have a court order or warrant, they may ask for a patient's health record to be disclosed voluntarily under the Data Protection Act 2018. In such cases, healthcare professionals may only disclose information where the patient has given consent, or there is an overriding public interest in line with the criteria in section 7.

Some police forces may use a standardised form developed by the National Police Chiefs' Council when requesting information from healthcare organisations (the form will not be used where there is a court order). The

9

police do not have to use this form but its use may help make the process of dealing with police requests more straightforward for healthcare professionals by ensuring the right information is included in the request and that the request is proportionate. The form will specify whether consent has been obtained. All requests should be provided in writing and signed off by a senior officer.

Family members and genetic information

The general principles of confidentiality apply equally to genetic information as to other information about health. Although genetic information frequently has relevance for family members, information about or provided by one patient should not be shared with others unless consent has been obtained (see section 3) or there is a legal requirement (see section 6) or an overriding public interest to justify disclosure (see section 7).

Complaints

When a patient complains about an episode of care, the matter cannot usually be investigated without some access to confidential information. Patients need to know this and should be told who will see the information, as well as being told about the safeguards in place. If they refuse to allow disclosure the complaint may not be able to progress, unless the information can be disclosed in the public interest (see section 7).

Patients sometimes involve their Member of Parliament (MP), or other elected representative, in the complaints process. Where the MP states in writing that they have the patient's consent for disclosure this may be accepted without further reference to the patient. Patients are also entitled to authorise relatives or carers to act on their behalf but, before responding, healthcare professionals should check that the patient consents to the disclosure.

When should information be withheld from access requests?

Certain information must not be disclosed when granting access to medical records. The most common examples are information which:

- is likely to cause serious physical or mental harm to the patient or another person; or
- relates to a third party who has not given consent for disclosure (where that third party is not a healthcare professional who has cared for the patient) and after taking into account the balance between the duty of confidentiality to the third party and the right of access of the applicant, the data controller concludes it is reasonable to withhold third party information.

The full list of exemptions and more detailed guidance on this topic can be found in our access to health records guidance.

Key resources

BMA – Access to health records
BMA – Focus on subject access requests for insurance purposes
GMC – Confidentiality: Disclosing information for employment, insurance and similar purposes

10

Secondary uses of information

What are secondary uses?

Secondary uses of information (or indirect care uses) are activities which contribute to the effective provision of health and care services and benefit the population (or groups of patients) through the development of new treatments and service efficiencies. These activities fall outside the scope of primary use because they are not related to the direct care of the individual patient.

Examples of secondary uses include research, commissioning, health service management, risk stratification, financial and national clinical audit, and education.

Will anonymised or pseudonymised information suffice?

Disclosure of anonymised or pseudonymised data (see section 11) will often satisfy a number of secondary uses and must be used where practicable.

When is explicit consent needed?

Explicit patient consent is needed for the disclosure of confidential information for secondary purposes, unless one of the following applies.

- the disclosure has been granted support by the Health Research Authority's Confidentiality Advisory Group (CAG) under section 251 of the NHS Act 2006 (in England and Wales) (see below);
- it is a disclosure made under the Confidentiality and Disclosure of Information Directions 2013, which provide a limited statutory basis for some specific disclosures where it is not possible to obtain explicit consent and where it is not feasible to anonymise data. These specific disclosures relate to the financial and management arrangements of the NHS, for example quality and outcomes framework reviews and investigating complaints; or
- the disclosure is otherwise required by law, for example notification of an infectious disease (see section 6).

What is section 251 of the National Health Service Act 2006 (England and Wales)?

Regulations under section 251 of the NHS Act 2006 permit certain disclosures to occur without a breach of the common law duty of confidentiality.

The Health Service (Control of Patient Information, COPI) Regulations can provide statutory support to enable health service management and medical research when it is not practicable to obtain consent and anonymised information cannot be used. Disclosures under these regulations are commonly referred to as having 'section 251 support'.

When presented with a request for confidential information with evidence that it has 'section 251 support', healthcare professionals can disclose the relevant information. It is not a legal requirement to disclose, however disclosures are encouraged due to the public benefit they serve.

Those wishing to access confidential information with 'section 251 support' must apply to the independent Confidentiality Advisory Group of the Health Research Authority.

In rare situations when there is a risk to public health, for example in a pandemic, the Secretary of State for Health and Social Care can use the COPI regulations to require certain information to be shared to help manage and control the disease.

10

In Scotland, those wishing to access confidential information for purposes which support the delivery of healthcare must seek advice from the Public Benefit and Privacy Panel for Health and Social Care. In Northern Ireland, the Privacy Advisory Committee advises healthcare organisations about access to information relating to patients.

Can patients opt out of 'section 251' disclosures?

Yes. In all but rare circumstances, 'section 251 support' is granted with the condition that patients must be able to opt out of the disclosure. The rare circumstances when an opt-out may not apply is when there are public safety concerns or the disclosure is for emergency public health reasons.

The national data opt-out (where patients in England can register to opt out of their confidential information being used for research or planning purposes) applies to 'section 251' disclosures in addition to any local mechanisms for opting out.

The national data opt-out (England only)

Patients in England can register a national data out-opt (NDO) to prevent the use of confidential information for research or planning purposes (subject to certain exemptions). Patients can set their preferences online. Postal and phone options are also available.

The NDO does not apply to disclosures:

- which are required by law, for example certain disclosures to NHS England under the Health and Social Care Act 2012;
- for participation in national screening programmes;
- for monitoring and control of communicable disease and other risks to public health;
- where explicit consent for a specific project has been obtained from
- the patient; or
- which are authorised by a court order.

UK GDPR requirements

For disclosures of confidential information to be lawful it is necessary to comply with both the common law duty of confidence and UK GDPR. Healthcare professionals should note that if consent is being sought to meet the common law this may not reach UK GDPR requirements for explicit consent which are higher than the common law. Instead, where these higher standards are not met, UK GDPR provides valid alternative legal bases which should be used in preference to consent. (See our separate guidance on GPs as data controllers under GDPR.) All secondary uses of confidential information must comply with the UK GDPR principles, including the requirement for transparency and the use of privacy notices which explain how confidential information is used and shared.

Key resources

GMC – Confidentiality: good practice in handling patient information
Health Research Authority – GDPR Guidance for researchers and study co-ordinators
NHS Digital – National data opt-out operational policy guidance

11 Anonymised and pseudonymised information

Disclosures of confidential information should be kept to the minimum necessary to achieve the purpose. Where possible, anonymised or pseudonymised information must be used if it will achieve the purpose of the disclosure.

A distinction must be drawn between anonymised information and pseudonymised information. There are important differences in how the two types of information can be disclosed.

Anonymised information

Information is anonymised if it does not identify individuals or does not enable individuals to be identified. The Information Commissioner's Office (ICO) says that if 'reasonably available' means can be used to re-identify individuals, that data will not have been effectively anonymised. A risk assessment of the means reasonably likely to identify an individual must be made considering the costs, time taken, and available technology. An example of anonymised data is national statistics which show the number of people attending A&E departments within a given time period.

When can anonymised information be disclosed?

'...disclosure by doctors or pharmacists to a third party of anonymous information, that is information from which the identity of patients may not be determined, does not constitute a breach of confidentiality.'
R v Department of Health, ex parte Source Informatics Ltd (2001)

Anonymised information can be freely used or disclosed without consent, including publication. Before disclosing anonymised information, healthcare professionals must be confident that the information is truly anonymised. The removal of direct identifiers such as name, NHS Number (or CHI), date of birth, and postcode can still leave information identifiable in some circumstances for example, rare diseases, drug treatments, or statistical analyses which have very small numbers. A combination of items increases the chance of identification.

Pseudonymised information

Pseudonymisation is a common technique for de-identifying information. UK GDPR considers pseudonymised data to be personal data unless the organisation holding the data does not have access to separate information that allows the re-identification of individuals.

Information is pseudonymised when obvious identifiers such as name, NHS Number (or CHI), or date of birth have been removed and replaced with a unique code or pseudonym which is held separately. However, the information is still about an individual person which increases the risk of re-identification. It might be possible, for example, to re-identify individuals if access is given to the 'key' to reverse the code or pseudonym or by linking the pseudonymised information with other sources of data. Pseudonymised information must be subject to technical and organisational safeguards to reduce the risk of re-identification of individuals.

11

When can pseudonymised information be disclosed?

When considering a disclosure of pseudonymised information, the environment in which the information is to be disclosed is of critical importance. To minimise the risk of re-identification of individuals, pseudonymised information must remain within a secure and controlled environment which has technical restrictions and contractual controls, for example:

- governance of the re-identification 'key' including ensuring that those who have access to the pseudonymised information do not have access to the 'key';
- contractual prohibitions on attempts at re-identification or linking to other data;
- confidentiality clauses in staff contracts, including sanctions;
- limits on access to the pseudonymised information; and
- use of encryption processes.

This list is not exhaustive and a risk assessment must be conducted, and documented, in each case. Healthcare professionals should follow the ICO's code of practice on anonymisation when considering disclosing anonymised or pseudonymised information (see key resources). Specialist advice might be needed when assessing the level of risk of re-identification and what level of controls should be in place to mitigate the risk.

Who can anonymise information?

It is not a breach of confidentiality if information undergoes anonymisation or pseudonymisation processes within the direct care team for a purpose that would be within patients' reasonable expectations (see section 3).

A lawful justification (see section 1) is required if confidential information is to be disclosed to a third party outside of the direct care team in order to undergo anonymisation or pseudonymisation processes.

Key resources

ICO – Anonymisation: managing data protection risk code of practice
Note that this guidance is out of date as it refers to the DPA 1998. The existing guidance should be followed while the updated version is awaited.

12

Security and avoiding inadvertent breaches

Keeping information secure

All healthcare professionals have obligations to handle confidential information responsibly and securely and protect it against improper access or disclosure. Protections are needed against both external threats such as cyber-attacks and internal threats such as accidental or deliberate breaches by staff.

There are some data security responsibilities which lie at senior organisational level in NHS trusts, local authorities, or with GP data controllers, although this will vary depending on the size and type of organisation. Those responsible must ensure compliance with national technical security standards and updates of software to protect IT systems from cyber threats.

All healthcare staff should know the identity of their Caldicott Guardian, Data Protection Officer, or Senior Information Risk Owner and know how to report a data breach or near miss.

General principles

To minimise the risk of unauthorised access to confidential information all healthcare staff must:

- not access a patient's record without a legitimate reason;
- avoid conversations in public places which may disclose confidential information, including online forums and social media;
- have appropriate training in confidentiality and data security matters;
- query the status of strangers on the premises; and
- wear ID where issued.

Digital or electronic records

In the case of digital or electronic records healthcare professionals must:

- always log out of any computer system when work is finished;
- not leave a terminal unattended and logged in;
- not share passwords or Smartcards with others;
- always clear the screen of a previous patient's information before seeing another;
- follow local policies on taking laptops or other portable devices home or offsite; and
- follow local policies on the use encryption and password protection.

Manual or paper records

Manual records must be:

- held in secure storage such as locked filing cabinets;
- formally booked out from their normal filing system;
- tracked if transferred, with a note of their current location within the filing system;
- returned to the filing system as soon as possible after use;
- kept closed when not in use so that the contents are not seen by others;
- inaccessible to members of the public; and
- kept on site unless removal is essential.

12

Telephone calls

Healthcare staff should confirm the identity of telephone callers if doubt exists that the caller is who they say they are, for example, by calling them back using an independent source for the phone number. Messages should not be left on answering machines to which others may have access or with family members.

Recorded telephone conversations are confidential in the same way as other information disclosed by patients for the purposes of receiving healthcare. Patients should be informed if their call may be recorded.

Texting patients

Many patients prefer their healthcare professionals to use text messages as a convenient way of communicating with them. It is acceptable to use text messages to communicate with patients about their care. Consent is not required to text patients about their care, however, to ensure compliance with data protection requirements, transparency information should be used to make patients aware of the types of information they can expect to receive by text, for example appointment reminders, repeat prescriptions or test results. The phone or device used to send the text messages must be secured in the same way as other electronic records to prevent accidental disclosure of the communication. Care should be taken to include the minimum amount of confidential information as possible in the message to reduce the risk of inadvertent data breaches.

Emailing patients

The NHS requires that confidential information held in digital or electronic form is encrypted before transmission. Great care must be taken to ensure that the correct email address is used, and that emails sent to more than one patient at once are bcc'd so that no recipient can see any of the other recipients' names or email addresses. The ICO has specific guidance on email and security which covers the use of bcc.

Sending confidential information to an unencrypted email address is not secure therefore the BMA advises that patients should be made aware of, and accept, the risks. This can be achieved by asking the patient to sign a disclaimer which includes:

- a checklist so that the patient can specify the information they are happy for the practice to send by email, for example, appointment reminders, appointment cancellations, or test results. The practice must abide by the patient's instructions;
- confirmation of the email address that the patient has provided – the practice is likely to be in breach of the UK GDPR if information is sent to the wrong email address;
- a statement that the patient is responsible for informing the practice of any change to their email address; and
- a statement that the patient is responsible for informing the practice of any change to their preferred method of communication, for example, if they no longer wish to receive information by email.

12

Processing and storing images

When remote consultations take place doctors can receive images, including intimate images, for clinical purposes. National guidance confirms that the approach to storing images should be the same as it would be for face-to-face interactions.

Key resources

DHNI – Code of Practice on Protecting the Confidentiality of Service User Information
NHS England – Data Security and Protection Toolkit
NHS Scotland – How the NHS handles your personal health information

13 Visual and audio images/ recordings

The advice in this section makes a distinction between disclosing images/ recordings made as part of a patient's care, and those made for non-patient care reasons, including with the intention of publication or broadcast.

When can recordings made as part of a patient's care be disclosed?

Visual and audio images/recordings made for clinical purposes are part of the medical record and are subject to the usual duty of confidentiality. These images can be shared for the direct care of a patient under implied consent (see section 3).

Adults with capacity

Images/recordings made as part of a patient's care should be treated in the same way as the rest of the medical record in terms of disclosures for secondary uses (see section 10), such as research or education and training. This means that explicit consent for disclosure will usually be required unless another lawful justification can be identified. Anonymised images can be disclosed for healthcare-related secondary uses, such as teaching or research, without consent. Those disclosing anonymised images, however, must be aware that apparently insignificant details may still be capable of identifying the patient and must be removed or redacted.

Healthcare professionals may wish to publish a recording of a patient which was made as part of their care. In these circumstances, explicit consent must be obtained if the patient is, or may be, identifiable. GMC guidance states that if the recording is anonymised, it is good practice to seek consent before publishing, bearing in mind the difficulties in ensuring that all the features of a recording that could identify the patient to any member of the public have been removed. Extreme care should be taken about the anonymity of such recordings before using or publishing them without consent in journals, other learning materials or any other media to which the public will have access.

The advice in earlier sections will apply when considering if disclosure of a recording is required by law (see section 6) the duty of confidentiality is set aside (see section 10) or the disclosure is justified in the public interest (see section 7).

The BMA has separate guidance on patients recording consultations (see key resources).

Adults lacking capacity

Medical research

If the image/recording cannot be anonymised, identifiable information can be disclosed for medical research provided it is in the best interests, or would benefit, the patient and is in line with relevant legislation. (Healthcare professionals should refer to the BMA's separate guidance on adults who lack capacity (see key resources) when considering disclosing identifiable information about adults lacking capacity for medical research.)

13

Education and training purposes
The law in relation to adults lacking capacity and the use of identifiable images/recordings for education and training purposes is untested. In the BMA's view it is difficult to see how such uses could be in the individual's best interests. Legal advice should be sought on a case-by-case basis for the use of identifiable images/recordings for reasons other than treatment and research.

When can recordings be made for use in widely accessible public media?

Publicly accessible media includes television, radio, online media and print.

Adults with capacity

The patient's explicit and written consent is required to make images/recordings intended for use in widely accessible public media. Explicit consent should still be sought even if it is considered that the patient is not identifiable, with the exception of certain intrinsically anonymous images, such as images of internal organs or images of pathology slides.

Patients should understand that, once material is published and in the public domain, it may be extremely difficult to withdraw it from circulation. Where a video recording has been made for a broadcast, doctors should check that patients understand that, once they have agreed to the recording being made for the broadcast, they may not be able to stop its subsequent use.

Adults lacking capacity

There are specific legal requirements in mental capacity legislation for making images/recordings of adults who lack capacity and using or disclosing such recordings. Legal advice should be sought in this area. The GMC states that in making audio or visual images/recordings for other secondary purposes, including images/recordings for publication, doctors must be satisfied that:

- the image/recording is necessary and benefits the patient or is in their best interests; and
- that the purpose cannot be achieved in a way that is less restrictive of the patient's rights and choices.

Key resources

BMA – Adults with incapacity Scotland toolkit
BMA – Mental Capacity Act Toolkit
BMA – Mental capacity in Northern Ireland toolkit
BMA – Patients recording consultations
GMC – Making and using audio and visual recordings of patients

14 Online complaints and the media

Responding to online complaints

Reading critical comments online from patients can be extremely upsetting and stressful. Many healthcare professionals feel strongly that patients forfeit their rights to confidentiality by posting on social media or speaking publicly and that they should be entitled to 'set the record straight' and correct any inaccuracies. In practice, healthcare professionals who do this would risk criticism and breach confidentiality. This principle applies even if the person replying to the complaint is not the member of staff complained about. Defending a colleague in a way that breaches confidentiality risks worsening the situation for both.

The advice of the GMC is that doctors should usually limit their public response to an explanation of the legal and professional duty of confidence that prevents them from commenting on specific cases, such as the one under discussion. This makes it clear that doctors do not have the right of reply and that readers should bear that in mind when reading the original complaint.

Any response must reflect the professionalism of healthcare staff. An inappropriate tone or impolite response may risk undermining public confidence in healthcare professionals.

Disclosures to the press

Under normal circumstances there will be no basis for disclosure of confidential information to the press. There will be occasions, however, when healthcare professionals are asked for information about individual patients.

For example, they may be asked to comment:

- on the condition of a celebrity patient. When the patient has the capacity to make decisions about disclosure, consent is essential before any information is released to the media. When the patient lacks capacity, legal advice should be sought; or
- after incidents involving harm to many people. During or after major disasters, for example a fire, road traffic accident, terrorist attack, or outbreak of infectious disease, it is important that requests for information are dealt with sensitively, while not breaching the confidentiality of patients.

Key resources

GMC – Responding to criticism in the media

15

Statutory restrictions on disclosure

Healthcare professionals are required by law to restrict the disclosure of some specific types of information. We have listed the most common examples below.

- *The Gender Recognition Act 2004 (UK)*
  Allows transgender people who have taken decisive steps to live fully and permanently in their acquired gender to apply for legal recognition of that gender. The Act makes it an offence to disclose 'protected information' (except in exceptional circumstances, for example, to comply with a court order) when that information is acquired in an official capacity. It defines 'protected information' as information about a person's application to the Gender Recognition Panel for gender recognition and a person's gender history after that person has changed gender under the Act.
- *The Human Fertilisation and Embryology Act 1990 (UK)*
  Protects confidentiality of the information kept by clinics and the Human Fertilsation and Embryology Authority (HFEA). Information can only be viewed by the clinic licence-holder and by staff or members of the HFEA (there are some additional limited exceptions to the restriction on disclosure, for example, disclosures to the Registrar General or a court). Disclosure of information which identifies the patient to another party without the patient's prior consent is a criminal offence. For more information see the HFEA's code of practice.

British Medical Association
BMA House, Tavistock Square,
London WC1H 9JP
bma.org.uk

BMA 20250040