



### Chapter 5 Confidentiality

#### Contents

- **Health and Social Care Information Centre (HSCIC) guide on confidentiality (page 192)**
- **Abuse and domestic violence (page 205)**
- **Dame Fiona Caldicott's review of information governance (page 193)**
- **Employment, insurance and other affairs (page 217)**
- **Disclosures under section 251 of the NHS Act 2006 (page 209)**
- **Statutory and legal disclosures (page 194)**
- **Anonymous information (page 193)**
- **Secondary uses of patient information (page 207)**

---

#### Health and Social Care Information Centre (HSCIC) guide on confidentiality (page 192)

In September 2013, the HSCIC published a guide to confidentiality in health and social care which clarifies how data should be used and shared. The code is available at: <http://www.hscic.gov.uk/configuideorg> (accessed 27 Nov 2013). Health and social care bodies processing confidential information must have regard to the guide.

**LATEST!**

The guide is centred around 5 key rules:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of individuals.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

A more technical document in the form of a Code of Practice will follow the guide.

---

#### Abuse and domestic violence (page 205)

In 2013 the BMA published guidance on vulnerable adults and the disclosure of confidential information. This is available at: <http://bma.org.uk/practical-support-at-work/ethics/mental-capacity/vulnerable-adults-and-confidentiality>

#### Dame Fiona Caldicott's review of information governance (page 193)

The findings of Dame Fiona Caldicott's *Information Governance Review: Information: to share or not to share*, were published in April 2013: <http://caldicott2.dh.gov.uk/> (accessed 17 May 2013). The aim of the independent review was to consider the balance between protecting confidential information and sharing it appropriately.

In relation to sharing information for direct care, the Review recognises that at times the health service has taken an overly cautious approach. A seventh principle has therefore been added to the existing six 'Caldicott principles'. This principle states that: 'the duty to share information can be as important as the duty to protect confidentiality'. The Review also emphasises that there should be 'no surprises' to the patient about who has had access to their medical record.

There are a number of chapters on use of data for secondary purposes, including research and commissioning and the governance arrangements in relation to linking data in safe havens, for example linking a patient's GP record with the hospital record to analyse a care pathway. The Review also includes a commitment to respecting patients' objections to confidential data being shared with the Health and Social Care Information Centre (HSCIC).



### **Employment, insurance and other affairs (page 217)**

The BMA's joint guidance with the Association of British Insurers (ABI) has been withdrawn and is under review. The BMA is aware that some insurance companies are now requesting full medical records rather than asking for a report from the applicant's GP as previously agreed with the ABI. In the BMA's view, requesting the full medical record is excessive as disclosures of information should be proportionate to the purpose for which the information is required. Under the Data Protection Act 1998 (DPA), however, patients are entitled to copies of their full medical record. Provided the patient has given explicit consent for the medical record to be shared with the insurer then doctors should comply with these requests. Decisions as to whether requests for information are excessive in terms of the DPA lie with the Information Commissioner's Office (ICO). Doctors with further enquires about medical information and insurance can contact the ethics department at: [ethics@bma.org.uk](mailto:ethics@bma.org.uk)

### **Disclosures under section 251 of the NHS Act 2006 (page 209)**

The Health and Social Care Act 2012 abolished the National Information Governance Board and created a National Information Governance Committee (NIGC) to replace it. The NIGC moved to the Care Quality Commission in April 2013. The ECC function moved to the Confidentiality Advisory Group (CAG) of the Health Research Authority (HRA) in April 2013. The CAG acts as a 'front door' to all applicants seeking section 251 approval. For research applications, the CAG will be responsible for approving applications, a role previously undertaken by the Secretary of State for health. The CAG will also consider and advise on non-research applications, although Secretary of State takes the final approval decision for these applications. Further information on the section 251 application process is available on the Health Research Authority website: <http://www.hra.nhs.uk/> (accessed 17 May 2013).

### **Statutory and legal disclosures (page 194)**

The Health and Social Care Act introduced new powers which allow the Health and Social Care Information Centre (HSCIC) to collect identifiable information in certain circumstances. These powers set aside the common law duty of confidentiality to seek patient consent. Under the Act, the HSCIC can 'require' identifiable information (or anonymised information) from providers if directed to do so by the Secretary of State for Health or NHS England; the HSCIC can also require information if it receives a 'mandatory request' from National Institute for Health and Clinical Excellence (NICE), Monitor or the Care Quality Commission (CQC). Providers have a legal obligation to comply with directions and mandatory requests from the HSCIC. The HSCIC will process the data it collects in a secure environment known as a safe haven. Identifiable data cannot leave the HSCIC unless there is an existing legal basis for disclosure. All data collections under the Act must comply with a statutory code of practice – to be published in 2013.

The first use of the powers under the Act is the care.data service. In conjunction with the Royal College of General Practitioners, NHS England and the HSCIC the BMA has produced guidance and FAQs on care.data which are available at: <http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records/care-data>

The guidance provides details on how patients can object. Patients can object in two ways:

1. To confidential data leaving the GP practice
2. To confidential data leaving the HSCIC

NHS England and the HSCIC also worked with the Information Commissioner's Office to provide further advice to GP practices on meeting their fair processing responsibilities under the Data Protection Act 1998 and their obligations to disclose data to the HSCIC under the Health and Social Care Act 2012. This is available at: <http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records/care-data>

### **Anonymous information (page 193)**

In November 2012, the Information Commissioner's Office (ICO) published a new code of practice on managing the risks related to anonymisation of data. The code is available at: [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/~media/documents/library/Data\\_Protection/Practical\\_application/anonymisation\\_code.aspx](http://ico.org.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Practical_application/anonymisation_code.aspx) (accessed 17 May 2013).

The code covers how personal data can be anonymised, for example for medical research, deciding when and how to release anonymised data, ensuring anonymisation is effective and different forms of disclosure.



The view of the ICO is that anonymisation does not have to provide a 100% guarantee to individuals' privacy in order for information to be disclosed, although the risk of re-identification through matching with other information must be 'remote'. In assessing the risk of re-identification, the ICO recommends using the 'motivated intruder' test. In other words, would a person who starts without any prior knowledge but who wishes to identify an individual be able to access resources and specialist expertise to enable re-identification.

### **Secondary uses of patient information (page 207)**

The BMA has produced guidance on dealing with requests for disclosure of data for secondary uses, for example from researchers or NHS managers. The guidance is available on the BMA website: <http://bma.org.uk/-/media/Files/PDFs/Practical%20advice%20at%20work/Ethics/releasingdataforsecondaryuses.pdf>