October 2013

British Medical Association position on the revision of the EU Data Protection Directive 1995/46/EC

The British Medical Association (BMA) is an independent trade union and voluntary professional association which represents doctors and medical students from all branches of medicine all over the UK. With a membership of over 152,000 worldwide, we promote the medical and allied sciences, seek to maintain the honour and interests of the medical profession and promote the achievement of high quality healthcare.

Overview

• The BMA welcomes attempts to increase the protection of personal data and recognises the need to update Directive 95/46/EC in light of advances in technology.

• The BMA welcomes the strengthening of provisions related to consent.

• The BMA stresses that the provisions relating to the use of data for historical, statistical and scientific research purposes must strike an appropriate balance between protecting confidentiality and allowing information to be used to facilitate important medical advancements.

Definition of consent

1. We support the EC’s proposal to clarify and strengthen the definition of consent and the requirement that it should be ‘explicit’, if it is to be relied upon for the processing of health data for purposes other than the direct provision of health care. The term ‘explicit’ is both well established and understood. In our view, the new definition will provide greater clarity as to whether consent has or has not been given. The definition should also include the requirement that the person has the capacity to understand what they are consenting to.

Imbalance between data subject and controller

2. The EC has proposed that consent should not provide a legal basis for the processing of data where there is a power imbalance between the position of data subject and controller. We believe that the key question is whether the relationship is coercive. Many patients may feel an element of power imbalance when they visit their doctor as the doctor holds clinical information which is necessary to treat the patient. The legislation must make it clear that the question of a potential power imbalance does not invalidate the consent a patient may give to their doctor.
Consent for sharing identifiable health data

3. Explicit patient consent must be sought when sharing identifiable data for purposes other than the direct provision of healthcare – e.g. for medical research and the commissioning of healthcare - apart from in the exceptional circumstances covered below. This is a well established principle in the UK which has been reinforced by the recently published Caldicott Review of information governance. If a patient subsequently withdraws consent for research, this must be respected. Further processing of this data for research would therefore be unlawful.

4. Where identifiable data are required and it is not possible to seek explicit consent, it is acceptable to use data for purposes beyond the direct provision of healthcare when the law provides an exception to allow data to be used for essential medical purposes which are in the public interest, and where anonymised or pseudonymised data will not satisfy the purpose. In the UK, Section 251 of the NHS Act 2006 provides for this exemption by allowing an independent body to approve the use of identifiable health data in such circumstances. The BMA strongly supports the provisions under Section 251 which allow core health service activities and important medical research to progress, whilst at the same time maintaining public trust through the independent scrutiny of applications for access to data.

One-time consent

5. The BMA supports the right of patients to take part in medical research and to be given increased access to information about research projects in which they may wish to participate. The health service should work towards making this information more readily available. However, the BMA would be opposed to the introduction of the concept of ‘one-time’ consent (or ‘broad’) consent for processing data for research purposes. Although this concept has an advantage in that it ensures that consent is sought in the first instance, it does present a number of difficulties in relation to how this might work in practical terms:

- Asking a patient to give ‘one-time consent’ for the sharing of information which does not yet exist would be fraught with difficulty.
- If one-time consent is given at the age of 18, the majority of people will not remember they have given consent at age 30 or 40. An individual may then hold very different views to those held at 18. This makes the consent given many years ago highly questionable.
- One-time consent becomes even more difficult in a situation where a patient undergoes medical treatment some years after giving consent which they consider to be highly sensitive (e.g. has a termination of pregnancy) and would not want disclosed.
- The introduction of one-time consent may lead to an increased reliance on the use of identifiable information for secondary purposes when, in many cases, anonymous or pseudonymous information would satisfy the purpose.
- Patients may be happy to give their consent for some research projects, but not others. If the consent is ‘one-time’ this may have the negative effect of people refusing consent for all research when, if offered more of a choice they would happily consent to some projects.

6. In addition, the BMA has concerns that the introduction of a new concept in relation to consent and information sharing might not be particularly helpful in light of the findings of the recent Caldicott review of information governance. The review highlighted that the variety of definitions and terms relating to information governance had lead to
confusion and misunderstanding amongst healthcare professionals about their legal duties and responsibilities. Given that the principles of implied consent and explicit consent are well established and generally well understood, the BMA would strongly suggest that policymakers avoid adding another layer to the concept of consent.

The use of anonymous/pseudonymous data

7. A key ethical and legal principle for sharing confidential health information is that anonymous information must always be used in preference to identifiable information. Those scrutinising applications under Section 251 of the NHS Act 2006 will consider whether the reason for seeking identifiable data could be met with the use of anonymised data. It is not necessary to seek consent for the use of anonymous/pseudonymous data.

Further processing of data which is already held for research purposes

8. Doctors must be able to carry out research on the data they legitimately hold, provided that this does not involve the disclosure of patients’ identifiable data. For example, a GP who collects data during the provision of care should be able to carry out research on the data within the GP practice. In the UK, an exemption exists in the Data Protection Act 1998 which allows for such an occurrence, subject to certain safeguards (Section 33).

The right to be forgotten

9. We believe that health records must be excluded from the right to be forgotten in the interests of the safe provision of care and for medico-legal reasons, such as when an audit trail is needed in case of a complaint.

Child’s consent in relation to information society services

10. The draft legislation proposes the age at which a child can consent as 13. This presents a number of difficulties, as there is significant disparity between nations regarding the age at which a child is judged to have the ability to consent. For example, in Scotland anyone aged 12 or over is legally presumed to be able to consent but this is not the case in the rest of the UK. In practice, a child’s competency to consent is deemed to be specific to the particular decision to be made and may vary depending upon matters such as the child’s previous experience of health care, social maturity, and other factors. These factors need to be taken into consideration if the age of consent is to be set within legislation.

Definition of pseudonymous data

11. The BMA believes that pseudonymous data are data which have had identifiers replaced through the use of unique codes or pseudonyms which do not reveal individuals’ ‘real world’ identity. Re-identification could occur if combined with other data or if access is given to the ‘key’ for reversibility, for example, when a group of patients’ data are processed using a pseudonym to link data from different care settings in order to filter those who are at high risk of hospital admissions. The healthcare professional would then use a key to re-identify the patients flagged as high risk so that appropriate interventions can be made. Using a pseudonym rather than the patient’s identity ensures that only those directly involved in the patient’s care know the identity of the individual, therefore protecting confidentiality.

12. The use of online pseudonyms - such as when logging onto websites - and the need to protect your pseudonymous profile (from advertising for example), in the same way that
your real identity is protected, is a separate issue. Any definition of the term would need to include an explanation of these two different usages as they require different sets of policy principles.

References

1 In 2012/13, Dame Fiona Caldicott carried out an independent review of information sharing to ensure an appropriate balance between the protection of patient information and the sharing of information to improve patient care. The findings were published in April 2013: https://www.gov.uk/government/publications/the-information-governance-review
3 https://www.gov.uk/government/publications/the-information-governance-review
4 The data must not identify individuals. With health data, identification may be possible even when obvious identifiers such as name, DOB, NHS Number are removed due to small numbers in cases of rare diseases, for example.