BMA

Requests for disclosure for secondary uses of data

The BMA regularly receives requests for advice and guidance from Local Medical Committees (LMCs) on releasing patient data for secondary purposes.[1] This document provides guiding principles to assist LMCs and practices in considering how to respond to these types of requests.[2] These principles can, however, be applied to all disclosures of data for secondary purposes.

1. In the first instance, it should be established whether the request for patient data is for secondary uses or for direct clinical care.[3] Examples of secondary uses include commissioning, health service management, risk stratification, financial and national clinical audit, research and public health surveillance.

2. Requests for data for secondary uses may be presented in different formats, for example, a data sharing agreement between the GP practice and a third party, a request from a Clinical Commissioning Group (CCG) or other third party access to GP practice records, requests from researchers and requests at a national level for data, for example, from NHS Digital.

3. Disclosure of anonymous data or de-personalised[4] data will often satisfy a number of secondary uses and must be used in preference to confidential patient information.[5] Consent for disclosure of anonymous or de-personalised data is not required. If a request is for confidential patient information and the GP practice feels that anonymised or de-personalised data would suffice, clarification should be obtained as to why identifiable data are required other than, exceptionally, where mandated by law, for example disclosures to NHS Digital under the Health and Social Care Act 2012.[6]

4. Explicit patient consent is needed for the use of confidential patient information for secondary purposes, unless the provisions in bullet point five apply. Patients can register a national data opt-out to prevent the use of their data for secondary purposes i.e. medical research and health service planning.[7] The opt-out will apply unless the information is required by law, there is an overriding public interest in disclosure or the disclosure is required for the monitoring and control of communicable diseases or other risks to public health.

5. Confidential patient information may be disclosed for secondary uses without explicit consent if:

    a. the disclosure of confidential patient information has been authorised by the Health Research Authority's Confidentiality Advisory Group (CAG) under section 251 of the NHS Act 2006 (in England and Wales)[8];
    b. it is a disclosure made under the 'Confidentiality and Disclosure of Information Directions 2013',[9] which provide a limited statutory basis for some specific disclosures where it is not possible to obtain express consent and where it is not feasible to anonymise data. These specific disclosures include secondary uses relating to the financial and management arrangements of the NHS, for example, Quality and Outcomes Framework (QOF) reviews, investigating complaints or suspected fraud[10]; or
    c. it is otherwise required by law.[11]

6. Any disclosure of confidential patient information must also meet the requirements of the General Data Protection Regulation and Data Protection Act 2018[12] therefore:
   a. data must not be retained longer than is necessary;
   b. the minimum amount of data required for the purpose should be disclosed;
   c. data must be held securely;
   d. information should also be obtained about whether the data will be stored in the UK, EU or outside the EU and GP practices should seek assurances that appropriate security and contractual arrangements are in place, this is likely to include evidence that the receiving organisation has carried out a Data Protection Impact Assessment[13]; and
   e. assurances should be sought (in writing) that information will not be transferred to a third party and it will only be used for the specific purpose for which it was disclosed.

7. A formal data sharing agreement or protocol may be advisable to ensure that both parties understand the limits and conditions of data sharing. Legal advice[14] and advice from the LMC may be required particularly when the data are being processed by a third party.

8. If there are doubts as to whether a disclosure should take place for secondary purposes then further guidance can be sought from Caldicott Guardians, indemnifying or regulatory bodies.

Further detailed guidance on information governance and data disclosure is available in the *Good Practice Guidelines for GP Electronic Patient Records*.[15]

References

1 The term 'secondary uses' or 'secondary purposes' refers to uses of patient data other than for the direct care of the patient.

2 Doctors should be aware of their obligations under the General Data Protection Regulation (GDPR) and consider each scenario on a case by case basis.

3 Direct clinical care refers to an exchange of information amongst members of the healthcare team providing care and treatment to the patient, for example when a patient is referred. Clinical audit undertaken by a member the team providing care to the patient is also considered part of direct clinical care.

4 Data that have had identifiers removed, however the information is still about an individual person. It might be possible to re-identify the individual if the data were not properly protected therefore de-personalised data must be subject to strict safeguards i.e. the data must remain in a secure environment with restrictions which prevent re-identification. Specialist advice should be sought when considering what level of controls should be in place.

5 Information from which a patient can be identified. Name, address and full postcode will identify a patient; combinations of information may also support identification, even if their name and address are not included.

6 NHS Digital has statutory powers under s259 of the Health and Social Care Act 2012 to require disclosures from providers in certain circumstances.

7 The online facility is available at: https://www.nhs.uk/your-nhs-data-matters/ (accessed 21 January 2019).

8 More information on the role of the CAG can be found at: https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/confidentiality-advisory-group/ (accessed 16 January 2019). There is no comparable legal framework in Scotland. In Northern Ireland, Regulations under the Health and Social Care (Control of Data Processing) Act 2016 are awaited.

9 *The Confidentiality and Disclosure of Information (GMS, PMS, and APMS) Directions 2013*

10 Patients must be provided with information which explains that their information will be used for financial or management purposes (and that they can object). Provision of this information in a 'privacy notice' is an existing requirement under the GDPR.

11 For example, notification of a known or suspected case of certain infectious diseases or certain disclosures to NHS Digital.

12 The BMA has separate guidance on GPs responsibilities under the GDPR: https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-data-controllers

13 The ICO's 'DPIA screening checklist' lists the factors which must be considered to determine the risks of a new project: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

14 BMA Law may be able to assist in reviewing or drafting data sharing agreements at discounted rate for members.

15 *The Good Practice Guidelines for GP electronic records* (2011) can be accessed at: https://www.gov.uk/government/publications/the-good-practice-guidelines-for-gp-electronic-patient-records-version-4-2011 (accessed on 16 January 2019)

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

BMA 20190107