**National Data Strategy open call for evidence**

**Response from the British Medical Association**

The BMA is a professional association and trade union representing and negotiating on behalf of all doctors and medical students in the UK. It is a leading voice advocating for outstanding health care and a healthy population. It is an association providing members with excellent individual services and support throughout their lives.

Our response focuses on the sharing and protection of confidential health data. The executive summary is highly relevant to 'Objective 1. To ensure that data is used in a way that people can trust'.

## Executive summary

### The purpose of medical records

- The primary purpose of medical records is to aid healthcare professionals in the direct care and treatment of individual patients.

- We recognise, and are supportive of, the many benefits which can be achieved through using health information for purposes beyond individual care; for example, medical research, health service improvement initiatives, quality audit and education of doctors and other healthcare professionals (often termed 'secondary uses' of data).[1]

### Importance of medical confidentiality

- Confidentiality is essential for the preservation of trust between doctors and patients. Patients should be able to expect that information which they give in confidence to their doctor will be kept confidential unless there is a compelling reason why it should not be.[2]

- This confidential relationship allows patients to be frank with their doctor, often confiding very personal, medical and non-medical information about themselves, safe in the knowledge that the doctor is under a legal and professional duty not to share the information (save in exceptional circumstances). If patients feel they are unable to be frank with their doctor it makes it impossible for the doctor to provide fully effective treatment – or patients may simply not visit their doctor at all.

[1] The BMA vision in relation to secondary use of data can be found here: https://www.bma.org.uk/collective-voice/policy-and-research/ethics/secondary-uses-of-data

[2] Such reasons include important statutory disclosures which require doctors to share information, for example, public health legislation requires that the appropriate authorities are informed about communicable diseases.

- There is, therefore, a strong public interest in maintaining a confidential health service so that patients will be encouraged to seek appropriate treatment and share information which is relevant to the provision of that treatment.

- The NHS is an extremely valuable data resource of life-long medical records. Confidentiality and trust must be maintained if effective use is to be made of these data. If datasets are incomplete due to patients withholding information or not seeking medical care this significantly undermines their usefulness therefore it is important to maintain a confidential health service both for individual patients and society at large.

- The particular sensitivity of, and obligation to protect, information shared in confidence between patient and doctor, is recognised in the common law duty of confidence – this goes above and beyond the protections in the General Data Protection Regulation and Data Protection Act.

- Within health, emphasis is placed on two useful rule of thumb principles which must be considered at the outset of any data sharing proposals:

    - that data should be shared in-line with patients' expectations; and
    - there should be no surprises for patients as to how their data are being used or shared.

  These important principles are prominent in the approach of the National Data Guardian for Health and Care.[3]

- Doctors also have professional duties of confidentiality which are set out in GMC (General Medical Council) guidance on confidentiality.[4]

**Responses to specific questions**

**Q1.1 How can organisations (private, public or third sector) demonstrate trustworthiness in their use of data?**

Within the health service there are well established principles, laws, professional standards and governance models for data collection and sharing. Any new systems for collecting or using healthcare data must have due regard to these arrangements, ensuring there are transparent procedures in place to safeguard and control access to data. There must be absolute clarity about how data can be accessed, by whom and for what purpose. When organisations routinely share data with third parties, maintaining a publicly available register of data releases can aid trust.

[3] https://www.gov.uk/government/organisations/national-data-guardian/about
[4] https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality

If public and patient trust is to be built, and maintained, it is important that both the government and individual organisations do not attempt to change established presumptions which are understood by both patients and healthcare professionals. This only serves to add to confusion and builds mistrust. If public trust is lost it would be extremely difficult to regain, and the advantages which can be gained through use of data will be lost.

Building trust through transparency and openness can include basic measures such as having clear data protection policies on websites. This sends a message to the public that the organisation takes its data protection obligations seriously.

Trustworthiness can be built through the early involvement of patients and public in data sharing plans. Within the field of medical research much work has already been done to promote collaboration between researchers and the public.[5] In 2018, the National Institute for Health Research (NIHR) and others published a set of national standards with the aim to increase the quality and consistency of public involvement in research and involving people at the earliest opportunity in the research plans.[6] This approach provides a good model to follow for all those who wish to use patient data, both within the NHS itself and outside the health service.

Organisations must view compliance with confidentiality and privacy laws as a continuing process that needs to be actively managed, rather than something to be done once and then forgotten. While risks to privacy can never be entirely eliminated, they must be effectively reduced and managed. Where bad practice is brought to light, organisations should challenge this.

**Q1.3. Are organisations (private, public or third sector) using personal data in ways that may damage trust?**

Unfortunately, there have been a number of recent examples within the health sector which have adversely affected trust:

- The MOU (Memorandum of Understanding) between the DHSC (Department of Health and Social Care), the Home Office and NHS Digital. The MoU permitted inappropriate data sharing between NHS Digital and the Home Office for immigration purposes which fell short of the standards of confidentiality set out in GMC guidance. The MoU was the subject of a Health Select Committee Inquiry and was subsequently suspended by the Government.[7]

- The collaboration between the Royal Free Hospital and Google *DeepMind* to develop the 'Streams' app. The ICO (Information Commissioner's Office) and the

[5] In addition, the majority of medical research projects in the UK also require ethics approval. Well established processes exist across the UK to ensure the relevant approvals and permissions are in place. https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/hra-approval/

[6] https://www.nihr.ac.uk/news/new-national-standards-launched-across-the-uk-to-improve-public-involvement-in-research/8141

[7] https://www.parliament.uk/business/committees/committees-a-z/commons-select/health-committee/inquiries/parliament-2017/mou-data-sharing-nhs-digital-home-office-inquiry-17-19/

National Data Guardian for Health and Care were critical of the data sharing which resulted in enforcement action by the ICO. [8] This example demonstrated that the potential benefits that new and innovative technologies can have on patient care must not be achieved at the cost of eroding privacy rights.

- There is an ongoing debate about the definition of 'confidential patient information'. The BMA and others are opposing attempts by the Government to categorise patients' demographic information as information which does not attract a duty of confidentiality. A statement of this sort would be contrary to professional and ethical guidance which treats names and addresses as being confidential within the health service, including where they are not linked to any clinical information.

**Q1.6. To what extent are people concerned about how data about them is used, stored and shared? Are some groups more concerned than others? Are there particular categories of data that raise more concerns than others?**

Issues concerning the use of health data and sharing with third parties have the potential to be contentious – particularly in circumstances where the benefits of sharing are unproven. It is important that patients understand not only why it is important to use data but that their concerns about privacy and confidentiality are responded to.

A recent YouGov survey provides an indication of some of the concerns which patients have and the challenges which must be addressed. The survey found that 71% of people were happy to share their health data for the benefit of healthcare in their local community provided it was anonymised.[9] This statistic is notable for the fact that a significant minority (29%) were not happy for anonymous data to be shared.

The results of the survey highlight two important considerations:

- That many people appear to be unaware of how the health service already uses patient data (in both anonymous and identifiable form) within the NHS, as well as by others such as medical researchers or commercial organisations; and

- Efforts need to be made to have a broad conversation with the public about how their data can be used for purposes beyond their care; what risks exist; and what safeguards and controls are in place to mitigate risk and protect confidentiality.[10] A prerequisite for these conversations is that organisations which handle patient data must be able to demonstrate they have a track record of trustworthiness and the ability to handle data securely.

[8] https://ico.org.uk/action-weve-taken/enforcement/royal-free-london-nhs-foundation-trust/
[9] https://www.sensynehealth.com/insights/yougov-survey-shows-uk-public-strongly-support-the-analysis-of-anonymised-nhs-patient-data 2081 adults took part in the survey between 11th – 12th March 2019.
[10] The 'Understanding Patient Data' initiative led by the Wellcome Trust is already doing important research into public views about the use of heath data.

The same survey also revealed attitudes towards the kind of organisations people trust with anonymous health data. This suggests a low level of trust in 'big tech' companies.[11] At the present time it appears that the public does not share the enthusiasm that many organisations have for partnership arrangements with 'big tech'. It remains unclear what factors, if any, may lead to a change in public attitudes towards acceptability. This requires further research and public debate – particularly in view of our response to the question below.

It is worth noting that the public place great trust in their GP. GPs have traditionally carried out the role of 'record guardian' for their patients – a role which, in our view, is fundamental to maintaining confidentiality and trust. Survey findings consistently demonstrate that GPs are seen as trustworthy guardians of health information.[12]

**Objective 6. To achieve alignment in government around data, with data shared and used cooperatively wherever appropriate.**

**Q6.6 Part 5 of the Digital Economy Act is designed to improve the use of publicly held information for specific purposes. How are organisations making use of the relevant powers, appropriately and effectively?**

We are aware that the Digital Economy Act includes a provision to set aside the common law duty of confidentiality to permit sharing health data amongst public bodies, including NHS Digital, without patient consent. We strongly opposed this legislation during its passage through Parliament – highlighting that the use of this power, especially in relation to identifiable health data, would permit an inappropriate and unprecedented sharing of confidential information. In response to our concerns, we received assurance from the Government that health bodies were, for the present time, excluded from the scope of the information sharing provisions. Furthermore, we received a commitment that any future decision to bring health bodies into scope would not take place without consultation with the health sector (including the BMA, GMC and National Data Guardian).

For further information, please contact:
Sophie Brannan, Senior Policy Advisor (Medical ethics) T: 0207 383 6816 | E: sbrannan@bma.org.uk

[11] 70% of respondents said would not be happy for data analysis of by a multinational 'big tech' company. Only 13% of respondents thought that such companies could be trusted to handle anonymised data. https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/rfiaqee3vv/Results%20for%20Lexington%20Comms%20(NHS)%20133%2012.3.2019.pdf

[12] https://www.bmj.com/content/362/bmj.k3488