The use of health information for medical research

AMRC’s position on health information, also known as patient data or health records, is:

• **AMRC supports the choice to opt-out of sharing health information beyond the purposes of a person's direct healthcare.** We believe that the public and patients must have the option to choose who has access to their personal health information.

• **We want to ensure that the public and patients are able to make an informed choice about sharing their personal health information.** The public need a better understanding of how the use of personal health information in research can transform care now and for future generations. At the same time, the public also need to understand the risks. There needs to be honesty about the fact that risks to privacy can never be eliminated entirely, although they can be reduced and managed.

• **The public need to feel that they can trust and have confidence in the health and social care system to collect, store and share their information with care and competence, and respect their wishes.** If the public do not trust the system, they will be unwilling to share health information for medical research and this will seriously hinder progress on new treatments and cures of diseases such as cancer, dementia, rare conditions and many more. **AMRC believes trust will be built by applying the 4Cs principles: choice, care, competence and clarity.**

The use of health information is crucial in medical research. Researchers use health information to develop understanding of disease and ill-health, discover new cures and treatments for patients; and improve the care provided by the NHS and other care organisations. **Health information enables researchers to save and improve lives, and it contributes to productivity and economic growth.**

The UK has a rich history of using health information for research purposes. The cradle-to-grave care provided by the NHS to our large, socially and ethnically diverse, population provides opportunities for research which are unparalleled internationally. This means that through our health information, researchers have opportunities to transform health and well-being for patients in the UK and across the world. For this reason **AMRC and its members support and encourage patients and the public to consent to sharing their data for the purposes of research and care planning.**

The case for data sharing must be made to the public. Medical research charities, research organisations, along with health and social care organisations need to take responsibility for making that case. The public need a better understanding of how the use of personal health information in research can transform care now and for future generations.

**Trust is essential: the 4Cs**

AMRC and its members recognise that an essential precursor to realising the opportunities of health information is for the public to have trust in the health and social care organisations and systems that collect, store, link and share their health information.
AMRC believes trust will be built by applying the 4Cs principles:

- **Choice**: let me decide who has information about me
- **Care**: treat my information with care
- **Competence**: handle my information according to rules
- **Clarity**: on who uses my information and for what purpose

**Choice: let me decide who has information about me**
AMRC supports the choice to opt-out of sharing personal health information beyond the purposes of a person’s direct healthcare. We believe that the public and patients must have the option to choose who has access to their personal health information, respecting their wishes of privacy.

The public and patients must be able to make an informed choice, including being given advice on what the future implications could be for medical research and their care if data is not shared. At the same time, the public also need to understand the risks. There needs to be honesty about the fact that risks to privacy can never be eliminated entirely, although they can be reduced and managed.

**Care: treat my information with care**
The public and patients must be able to trust that their health information is collected, stored, linked and shared securely.

Health and social care organisations must meet the data security standards set out in Dame Fiona’s Caldicott’s ‘Review of Data Security, Consent and Opt-Outs’. Wherever possible, de-identified and anonymised data should be used instead of personal identifiable data to minimise risk.

**Competence: handle my information according to rules**
The public and patients must be able to trust that their health information is managed at all times according to data protection laws and other relevant guidance.

The health and social care organisations, safe havens and all users of data should be held to account for their handling and use of the data. Governance requirements need to be clear and adherence monitored effectively. Sanctions must be applied transparently to those who have broken the rules.

**Clarity: on who uses my information and for what purpose**
There needs to be better clarity on which types of organisation will be able to access personal health information and for what purposes. This should be clear for all stakeholders, including the public, to understand and there should be no surprises emerging in future years.

A coherent, single overarching governance framework for personal health information is needed. The fragmentation and complexity of the current information governance arrangements in the NHS hampers accountability and the ability to communicate effectively to the public.