DRAFT – November 2014

'Consent for Consent'

Introduction:

Consent for Consent can be described as: consent to access medical records in order to identify eligible research participants to approach to see if they would like to participate in a research study. Commonly such access is undertaken by research professionals who are not members of the clinical care team. The issue is whether consent is needed to access the medical records in this way and for this purpose.

This document aims to outline the complex and untested legal situation with regard to accessing, without consent, personal identifying information by research professionals who are not part of the clinical care team, and makes recommendations on how to proceed in this complicated area. It summarises previous MRC guidance (MRC Ethics Series: Personal Information in Medical Research), Department of Health guidance on disclosure (Confidentiality: NHS code of Practice), British Medical Association Guidance on Secondary Uses of Patient Information, and advice from the Information Commissioner's Office.

MRC Recommendations:

The MRC recommends that all the legal and ethical information below be considered in the context of individual projects. The key points to consider are:

- Whether consent is really not feasible – practicalities of contacting those involved
- Whether patients are aware that information may be disclosed
- Grounds for disclosure – the importance of the research activity, public good/benefits to society
- Nature of the information to be disclosed – e.g. the sensitivity of the information
- Safeguards in place – ethical review, NHS R&D permission, researcher has equivalent standards of confidentiality as clinical care team

The potential risks to patients, researchers and medical practitioners must be considered before medical records are accessed by research professionals who are not members of the clinical care team, without consent.

In many situations the infringement of confidentiality will be minimal, for example if records are accessed by trained professionals with an equivalent duty of confidentiality as members of the care team. The justification for the study would need to be considered by a Research Ethics Committee and NHS R&D management permission would need to be in place, and where appropriate approval from the HRA Confidentiality Advisory Group (HRA CAG).

Access to patient records to identify research participants is often considered in research proposals. It would therefore be advisable for all organisations that maintain patient records to ensure that patients are aware that research professionals with the same duty of confidentiality as NHS employees may see patient notes, and that patients may be invited to participate in research projects.

Summary of existing guidance:

Extract from MRC Ethics Series: Personal Information in Medical Research

Common Law
In the UK, the confidentiality of personal information is addressed primarily in Common Law. **In Common Law, anyone who receives information must respect its confidentiality** (that is, not disclose it without consent or other strong justification) if they receive it on the understanding that it is confidential, or in circumstances where there is an implicit expectation that they will not reveal it to anyone else. But while Common Law establishes some core principles, **it does not specify when confidential information may or may not be disclosed to others in research** or most other activities. **Individuals and organisations using confidential information have to take responsibility for deciding what is justified and acceptable on a case by case basis.**

Common Law enshrines the principle that to disclose confidential information about a living person without consent is, generally speaking, to wrong an individual. **In law, any information doctors have about their patients must be regarded as confidential**, even addresses that might be publicly available elsewhere, because the information is given with the expectation that it will not be passed on. **Disclosing confidential personal information does not have to cause direct harm or distress for it to be unlawful** – any unjustified use of confidential information that weakens trust in the doctor-patient relationship could also be seen as actionable.

However, **Common Law also recognises that it can be in the public interest for doctors to disclose confidential personal information**, and that the **nature and scale of disclosure has to be balanced against the benefits to society**. Interpretations of this balancing judgement may vary, and there are few court rulings relevant to the sorts of limited disclosures involved in research. The legal advice to MRC is that the legality of using confidential information in research without consent, could only be judged on a case by case basis, taking into account:

Necessity – were there alternative, practical ways of conducting the study, which would have allowed consent to be obtained?
Sensitivity – how much did the information reveal about the individual, and was it particularly likely to lead to worry or distress, or damage the doctor-patient relationship?
Importance – was the research well designed, and likely to make a significant contribution to knowledge in the area?
Safeguards – was the amount of information disclosed as small as possible? Were all reasonable steps taken to guard against unintended leaks of information and to maintain trust? Was the risk that the study or its findings might cause distress minimised?
Independent review – was the justification for the research reviewed by a Research Ethics Committee?
Expectations – if explicit consent was not possible, were there reasonable efforts to make people involved aware of how medical records were used, so they had an opportunity to raise any special concerns?

Despite the fact that research projects may have been approved by a Research Ethics Committee, and authorised by a Health authority or Trust, **individual doctors remain accountable for their use of their patients' information.** The same applies to those who receive confidential information: **members of a research team must always be aware that they share a similar duty of confidence to doctors**, and that revealing any personal information they hold without good reason – whether resulting from neglect, ignorance, or malice – is potentially actionable.

Data Protection Act 1998[1]

The Data Protection Act 1998 is based on the concept of fair processing.
The Research exemption, Section 33(5) states that …personal data are not to be treated as processed merely because the data are disclosed: (a) to any person, for research purposes only…

In the Act this relates to sub-sections 2-4 of section 33; this means the following in practice for data disclosed for research purposes[2]:

- The 2nd Data Protection Principle[3] does not apply, so personal data can be disclosed for research even if it is incompatible with the purposes for which is was obtained.
- The 5th Data Protection Principle does not apply, so data disclosed for research can be kept for longer than is necessary for the purpose for which it was obtained.
- That Section 7 of the Act does not apply, so data subjects do not have rights of access to data that is disclosed for research purposes.

The Act also states that the use of medical records is acceptable under the clauses of the Act, however this does not necessarily mean it is lawful or fair: it is also to be consistent with Common Law on confidentiality, and with general concepts of fairness.

Confidentiality: NHS Code of Practice (Department of Health)

The Department of Health guidance, Confidentiality: NHS Code of Practice, gives advice to NHS staff on disclosure of personal information and places the emphasis on whether consent could be sought, and proportionality based on public good and risk to the patient. Some relevant extracts from the guidance include the following:

Preventative medicine, medical research, health service management, epidemiology etc are all medical purposes as defined in law. Whilst these uses of information may not be understood by the majority of patients, they are still important and legitimate pursuits for health service staff and organisations.

However, the explicit consent of patients must be sought for information about them to be disclosed for these purposes in an identifiable form unless disclosure is exceptionally justified in the public interest or has temporary support in law under section 60 of the Health & Social Care Act 2001….

…Similarly, when the public good that would be served by disclosure is significant, there may be grounds for disclosure. The key principle to apply here is that of proportionality. Whilst it would not be reasonable and proportionate to disclose confidential patient information to a researcher where patient consent could be sought, if it is not practicable to locate a patient without unreasonable effort and the likelihood of detriment to the patient is negligible, disclosure to support the research might be proportionate. Other factors e.g. ethical approval, servicing and safeguards, anonymisation of records and/or clear deletion policies etc might also influence a decision on what is proportionate. It is important not to equate "the public interest" with what may be "of interest" to the public…

…In some exceptional circumstances, where the research subject is of such significance or a patient cannot be located in order to seek consent, the public interest may justify disclosure…

…There are situations where consent cannot be obtained for the use or disclosure of patient identifiable information, yet the public good of this use outweighs issues of privacy. Section 60 of the Health and Social Care Act 2001 currently provides an interim power to ensure that patient identifiable information, needed to support a range of important work such as clinical audit, record validation and research, can be used without the consent of patients…

[Please note Section 60 of the Health and Social Care Act 2001 has been superseded by Section 251 of the NHS Act 2006.]

[1] There is ongoing debate about the interpretation of Section 33 of the Data Protection Act 1998. Academy of Medical Sciences report 'Personal data for public good: using health information in medical research'
[2] Based on advice from the Information Commissioner's Office (www.ico.gov.uk)
[3] See Annex for the Data Protection Principles

British Medical Association Guidance on Secondary Uses of Patient Information

This guidance outlines the governance of the use of information about individual patients, including Data Protection Act 1998, Human Rights Act 1998, Health and Social Care Act 2001, The Common Law, Professional Standards, and Policies and Organisational Standards. It states that:

It is important to note that the legal position on confidentiality is complex. Legal responsibilities in respect of confidential information cannot be gleaned from common law and statute alone, and health professionals must look at the overall effect of the law, not each aspect in isolation... Doctors who are uncertain about the application of the law in a particular case should seek legal advice. Doctors must also ensure that their actions comply with the guidance issued by the General Medical Council...

...In the absence of patient consent or anonymisation any decision as to whether identifiable information is to be shared with third parties must be made on a case by case basis and must be justifiable in the "public interest"...
...The General Medical Council also provides guidance to doctors on what they must consider prior to making a disclosure in the public interest.
GMC advice on disclosures in the public interest:
"Personal information may be disclosed in the public interest, without a patient's consent, and in exceptional circumstances where patients have withheld consent, **where the benefits to an individual or to society of the disclosure outweigh the public and patient's interest in keeping the information confidential.** In all cases where you consider disclosing information without consent from the patient, you must weigh the possible harm (both to the patient and the overall trust between doctors and patients) against the benefits which are likely to arise from the release of information..."

The BMA...recognises that in the context of secondary use of information, public interest must be a balance between individuals' and society's rights and claims to confidentiality and the rights and claims of the whole of society to better health and to protection against threat to ill health. Any disclosure of identifiable information must be proportionate to the anticipated benefit and subject to good governance rules. To make such an evaluation requires consideration of:

- The degree of disclosure and the expected benefits for society
- The degree of intrusiveness for the patient
- The level of public awareness and acceptance of the disclosure

Please note that the Health and Social Care Act 2001 has been superseded by the NHS Act 2006.

Governance of access

In England and Wales, under Section 251 of the NHS Act 2006 (formerly section 60 of the Health and Social Care Act 2001), the HRA Confidentiality Advisory Group (HRA CAG) can give approval to use identifiable information without consent. Health professionals have to make a strong argument that their work is in the public interest, needs identifiers and that it would not be feasible or appropriate to anonymise or get patient consent. In Scotland and Northern Ireland, Privacy Advisory Committees have been established; however, there are no equivalent statutory arrangements.

There are a number of activities, such as the development of national IT frameworks through Connecting for Health (England – in particular the Secondary Uses Service), Informing Healthcare (Wales) and the Emergency Care Summary (Scotland) as well as Government's developing strategy on the sharing of personal information across Government agencies. All these initiatives are expected to have an impact on the environment for the use of personal health data in research.

In August 2007, the care Record Development Board working group published their report, 'Report of the Care Record Development Board Working Group on the Secondary Uses of Patient Information'. The aim of this group was to advise the Care Record Development Board and through it the National Programme for IT, on how the potential for the NHS Care Records

Service to support research, population health and management can be realised in compliance with the NHS Care Record Guarantee for England and the secure and ethical use of patient records.

Annex

Data Protection Principles

Data controllers may only process personal data if they do so in compliance with the Eight Data Protection Principles set out in the Act. These principles require controllers to ensure:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, al least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner that is incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or purposes.

6. Personal data shall be processed in accordance with rights of the data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.