Connected Health Cities IG Working Group

Consent Briefing Paper

Background

Over the past months there have been several discussions within the CHC regarding 'consent'. The term 'consent' in these discussions refers to consent for data sharing and processing. Furthermore, generally we are referring to consent required for the common law duty of confidentiality.

Generally, in the CHC projects we are concerned with the basis for processing data for purposes other than direct care.

To process personal confidential data (personally identifiable data) you must meet the common law duty of confidentiality. Options for this are:

- with the **consent** of the individual concerned.
- through statute, such as the powers to collect confidential data in section 251 of the NHS Act 2006 and the powers given to the Information Centre in the Health and Social Care Act 2012
- through a court order, where a judge has ordered that specific and relevant information should be disclosed and to whom; and
- when the processing can be shown to meet the 'public interest test', meaning the benefit to the public of processing the information outweighs the public good of maintaining trust in the confidentiality of services and the rights to privacy for the individual concerned.

In addition to having one of these legal bases the processing must also meet the requirements of the Data Protection Act and pass the additional tests in the Human Rights Act.

Often there is a legal basis for processing the data under the DPA even though the common law duty of confidentiality has not been met. This requires that one of the conditions from schedule 2 and schedule 3 of the Act are met. However, if we are also relying on consent as a legal basis for processing data under the DPA (or in future under the UKs new Data Protection Act which will ensure that we meet the requirements of the General Data Protection Regulations) we must ensure that this is clear and that the requirements for valid consent under GDPR have been met.

The aim of this paper is to consider the implications of seeking consent or adopting an opt-out approach and to discuss the role that the IG Working Group should take in shaping the approach that the CHCs adopt and to agree any work to be undertaken by the HUB.

Terminology and Definitions

Previous discussions have centred around both consent and opt-out, sometimes confusing their respective purpose. It would therefore be useful to ensure that we all adopt the same terminology and understanding. To that end the following definitions are proposed:

Consent*[1]*: *The informed agreement for something to happen after consideration by the individual. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. In the context of consent to share confidential information, this means individuals should know and understand how their information is to be used and shared (there should be 'no surprises') and they should understand the implications of their decision, particularly where their refusal to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.*

Explicit consent*[2]*: *Explicit consent is unmistakeable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. A patient may have capacity to give consent, but may not be able to write or speak. Explicit consent is required when sharing information with staff who are not part of the team caring for the individual20. It may also be required for a use other than that for which the information was originally collected, or when sharing is not related to an individual's direct health and social care.*

Implied consent: *Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed. Examples of the use of implied consent include doctors and nurses sharing personal confidential data during handovers without asking for the patient's consent. Alternatively, a physiotherapist may access the record of a patient who has already accepted a referral before a face-to-face consultation on the basis of implied consent.*

Opt-out: *The option for an individual to choose not to allow their data to be used for the purposes described. This does not constitute consent to process data for 'secondary' purposes*

Consent

Patient consent is required to provide a legal basis under the common law duty of confidentiality for processing personal confidential data (personally identifiable data). For the purposes of direct care, where patients have been informed of the extent of data sharing, implied consent can be relied upon. For all other purposes explicit consent will be required.

A legal basis for processing data is also required to meet data protection laws but this is normally achieved by meeting one of the conditions in Schedule 2 and in Schedule 3 of the Data Protection Act 1998. Similarly, the GDPR sets out conditions for lawful processing, and further conditions for processing special categories of personal data (Articles 6 and 9). Therefore, it remains likely that consent will not be required to provide a lawful basis under GDPR.

Consent is not required for processing anonymised patient data, nor is it required for processing pseudonymised patient data where the controls imposed (through data sharing arrangements and safeguards) render it non-personal data. Although, it should be noted that consent would be required if the data is provided to a third party to link and pseudonymise it for a CHC project as the duty of confidentiality is broken when the data is supplied to the third party.

It is a principle under DPA (and adhered to by CAG) that if consent is sought from a patient and not obtained (e.g. because of a failure to respond to correspondence seeking consent then the patient's

[1] Your Data: Better Security, Better Choice, Better Care. Government response to the National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs and the Care Quality Commission's Review 'Safe Data, Safe Care'
[2] Information to Share or not to Share: The Information Governance Review (Caldicott 2)

personal confidential data (personally identifiable data)) it cannot then be processed by seeking an alternative legal basis such as s251.

It should be noted that the approach to pseudonymised data under GDPR changes slightly from DPA as it is likely that pseudonymised data will still be considered to be personal data and to fall within the GDPR. Various national bodies are exploring the implications this will have after GDPR comes into force in May next year. Advice from the IG Alliance is awaited (expected later this month or early next month) and the ICO are believed to be amending their Anonymisation Code of Practice to include any additional safeguards required to allow pseudonymised data to be considered anonymised and therefore not subject to the restrictions of the Data Protection law.

Purposes for seeking Consent

Generally, for CHC projects, data providers will need a lawful basis to provide personal confidential data (personally identifiable data) to the project.

However, they may also require consent for other purposes such as;

- to approach patients to seek their participation in other research studies
- to enable access to link the data with other healthcare records about the patient that might be held by other organisations.
- to contact patients or their clinicians if, during the research or service evaluation, something is identified that may be urgent/harmful to the patient's health/welfare.

The consent sought should be granular and should specify each of the full range of purposes the data is to be used for to enable / allow patients to consent to each purpose separately. The consent sought should attempt to anticipate future uses, for example is the research likely to want to link with other records in future? It is also important to strike a balance between being specific about the data uses and avoiding being too specific so that the consent is not future proofed. For example: seek consent for linkage with other heath records held about the patient instead of seeking consent to link with HES data held by NHS digital.

In seeking consent, it is important that the patients are provided with an information sheet which clearly explains in plain English why their consent is being sought and provides details of the project.

Research participants (e.g. patients that have the condition which is the subject of the research) should be used to review information sheets and consent documents to ensure that they are understandable.

The UK Biobank resources page provides examples of patient's information sheets and consent forms:

http://www.ukbiobank.ac.uk/resources/

The Health Research Authority provides guidance in seeking consent which can be found here:

http://www.hra.nhs.uk/resources/before-you-apply/consent-and-participation/consent-and-participant-information/

National opt-out

It is important to make clear the distinction between consent and opt-out (or dissent). Providing patients with an opportunity to opt-out does not provide a legal basis for processing personal

confidential data (personally identifiable data) under the common law duty of confidentiality. It only provides an opportunity for patients to express their wishes that their personally identifiable data is not used in certain circumstances.

The NDG recommended a new national opt-out to give people a clear choice about how ***their personal confidential data is used for purposes beyond their direct care***. The Government response to this recommendation has endorsed the NDG's proposed national optout and intend to implement it. The national opt-out will clarify how people can opt out, recognising that information will flow where there is a mandatory legal requirement, an overriding public interest or other exceptional cases. Individuals will be able to make their choice known online as well as in person.

In effect, as the processing of personal confidential data (personally identifiable data) relies on either patient consent or S251 support to provide a legal basis for the common law duty of confidentiality, the national opt-out will only apply (with few exceptions) to data processed under s251 support.

It is not yet clear how the national opt-out model will work: NHS Digital will collect patients recorded opt-out wishes but they have yet to describe how these will be enforced for data that is not supplied by NHS Digital themselves.

Currently, the Confidentiality Advisory Group usually requires any organisation seeking S251 support to ensure that data providers allow patients to opt-out locally of the specific use to which their data is being processed under the S251 support.

Principles to be applied in seeking consent

This would suggest a number of principles need to be applied by the CHC:

- Consent is not required (currently[3]) and should not be sought for processing anonymised or pseudonymised data (unless a third party is involved in linking and pseudonymising the data).
- Where consent is to be sought for processing personal confidential data (personally identifiable data) the patient must be informed of the purposes for which their data will be used; who will be involved in processing their data (including any data processing suppliers); and how long it will be retained for. The consent should be recorded and should be auditable.
- Under the DPA and in future under GDPR it is likely that a legal basis can be found using the conditions set out within the Act.
- The national opt-out does not need to be applied to anonymised or pseudonymised data.
- Processing of personal confidential data (personally identifiable data) that relies on s251 support for a legal basis will need to honour the patients' national opt-out wishes and may also need to introduce a local opt-out process for that particular project.
- Patient information must be made available in various ways to ensure that patients are made aware of the purposes for which their data is being used so they can either provide their explicit consent if it is being sought OR register an objection through opt-out if there is another legal basis for processing such as s251.

[3] This may change if pseudonymised data is considered to be personal data under GDPR