Ensuring a lawful basis of sharing for the South West London Interoperability Programme

This paper has been updated to take into account comments at the February 2018 SWL Information Governance Working Group, the DCC STP IG Leads Steering Group and a meeting between the IG Lead representatives from the SWL Local Authorities.

Background

To ensure compliance with privacy and confidentiality law, there must be a lawful basis to share personal data between providers for the purposes of direct care. How this is achieved and what lawful basis is decided on was the subject of discussion at the January 2018 SWL IG Working Group. This paper will review the current and upcoming legislation privacy and confidentiality law and provide options on approaches that could be taken on the SWL Interoperability Programme. This paper will only review insistences of sharing data for direct care where it is considered the patient has capacity. Where a patient/service user does not have capacity, or sharing is considered necessary for reasons of safeguarding or public interest local policies reflecting national guidance should be followed.

Data Protection and Common Law Duty of Confidentiality

Data Protection Act 1998

To process personal data in the United Kingdom, there must be a lawful basis under the Data Protection Act 1998. These are found within Schedule 2 of the DPA 1998. Sensitive personal data, of which health data falls within, must also meet an additional lawful basis, found in schedule 3.

Under the Data Protection Act 1998, the common conditions used to process health personal data are either:

- Condition 5(d) of Schedule 2 and Condition 8 of Schedule 3 (where the processing is for medical purposes); or
- Condition 4 of Schedule 2 and Condition 3 of Schedule 3(where the processing is in the vital interest of the data subject).

'Medical purposes' is defined in DPA 1998 as '*includes purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.'*[1] The Health and Social Care Act 2001 subsequently added social care to be included within the definition of medical purposes[2].

[1] Data Protection Act, Sch 3, Para 8(2)
[2] Health and Social Care Act 2001, S 60, Para 10

General Data Protection Regulation and Data Protection Act 2018

May 25th 2018 will see the implementation of new data protection legislation across Europe which will be transposed into UK law by a new Data Protection Act. Like the 1998 Act, GDPR will require both a lawful basis to process personal data and an additional basis to process special category personal data[3], of which health and social care data continues to be one.

Under GDPR, the common basis that can be used to process health and social care personal data will be:

- Articles 6(1)(e) (public task) and 9(2)(h) (medical purposes); or
- Articles 6(1)(d) (vital interests) and 9(2)(c) (vital interests)[4]

Medical purposes is defined in GDPR as '*preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3'*

Whilst the scope is therefore defined, unlike DPA 1998 where the definition is preceded by 'includes', social care is explicitly mentioned which leaves no ambiguity that the processing of such personal data can be considered alongside health data.

As a further safeguard when processing health and social care personal data using Article 9(2)(h), Article 9(3) requires that that processing is undertaken by, or under the responsibility of individuals who have an obligation of confidence. The Data Protection Bill [HL] interprets this as circumstances which include where processing is carried out:

(a) by or under the responsibility of a health professional or a social work professional[5], or
(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law[6]

Common Law Duty of Confidence

The common law duty of confidence has arisen from case law, not statute, and arises where one person discloses information to another in circumstances where it is reasonable to expect that the information is held in confidence. As well as being required under case law, medical professionals have the requirement in their respective code of conducts and NHS employment contracts.

Due to fact the duty is based on case law, interpretations of the law must be relied on and there is no legislation behind it. Two of the leading interpretations in a health environment are found in the Department of Health's Confidentiality Code of Practice (2003) and the GMC Confidentiality Guidance (April 2017).

Both these references suggest that, when sharing for direct care[7], the implied consent of the patient/service user may be relied upon with the assurance certain conditions have been met.

---

[3] Formerly Sensitive Personal Data under DPA 1998
[4] Defined as 'essential for life of the data subject or another natural person' in Recital 46 of GDPR
[5] Health and Social Care professionals are defined in Part 7, Section 197 of the Data Protection Bill.
[6] Data Protection Bill [HL], Part 2, S11, Para 1(a)
[7] Referred to as 'healthcare purposes' in Department of Health Confidentiality Code of Practice as *'These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided.'*

In the Department of Health Code of Practice, these are that:

'Where patients have been informed of:

a. the use and disclosure of their information associated with their healthcare; and
b. the choices that they have and the implications of choosing to limit how information may be used or shared;

then explicit consent is not usually required for information disclosures needed to provide that healthcare.'[8]

In the GMC Guidance, these are:

'You may rely on implied consent to access relevant information about the patient or to share it with those who provide (or support the provision of) direct care to the patient if all of the following are met.

a. You are accessing the information to provide or support the individual patient's direct care, or are satisfied that the person you are sharing the information with is accessing or receiving it for this purpose.
b. Information is readily available to patients, explaining how their information will be used and that they have the right to object. This can be provided in leaflets and posters, on websites, and face to face. It should be tailored to patients' identified communication requirements as far as practicable.
c. You have no reason to believe the patient has objected.
d. You are satisfied that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect.'[9]

Both of these therefore put a responsibility on the organisations sharing data for direct care to ensure patient/service users are fully aware of sharing and can object to the sharing at any time.

Two further interpretations that span across both Health and Social Care are the '*Information: To share or not to share?'* report by Dame Fiona Caldicott; and the Health and Social Care Information Centre (now known as NHS Digital) '*Guide to Confidentiality in Health and Social Care'.*

Dame Fiona Caldicott states in her 2013 report that '*…the health and social care professional is able to rely on 'implied consent' when sharing personal confidential data in the interests of direct care, as long as the patient does not object, or has not already done so.'.*

The Guide to Confidentiality in Health and Social Care states:

'When an individual agrees to being treated by a wide care team it creates a direct care relationship between the individual and the professional, as well as their team. In these situations it is reasonable for staff to assume that the individual is also agreeing to confidential information about them being shared by the care team[10]*.'*[11]

The Health and Care Professionals Council, who regulate a variety of professions including social workers and occupational therapists, support the use of implied consent for direct care in their confidentiality guidance, stating

[8] Department of Health, *Confidentiality: NHS Code of Practice,*(7 November 2003) para 15
[9] General Medical Council, *Confidentiality: Good practice in handling patient information,* (25 April 2017) paragraph 28
[10] Examples of individuals within a 'care team' are named to include 'social workers, doctors, nurses, laboratory staff, social care staff, those that provide specialised care and the administrative staff who support care provision.
[11] Health and Social Care Information Centre, *A guide to confidentiality in health and social care,* (September 2013) Page 13

that *'Most service users will understand the importance of sharing information with others who are involved in their care or treatment and will expect you to do so, so you will normally have implied consent to do this.'.* This is caveated by three requirements that should be met before sharing with implied consent, these being:

'– it is necessary to provide the information;
– you only disclose the information that is relevant; and
– the professional receiving the information understands why you are sharing it and that they have a duty to keep it confidential.'[12]

Health and Social Care (Quality and Safety) Act 2015

The Health and Social Care (Quality and Safety) Act 2015 introduced a duty to share information where it was likely to help facilitate care to an individual and was in their best interest[13]. This duty does not require explicit consent to be gained from patient/service users, and states that the duty doesn't apply where the patient/service user has objected, or would be likely to. It goes on further to state that no sharing must be inconsistent with both the DPA 1998 and common law duty of confidentiality, to which duty is to share for help facilitate care (to include direct care) means implied consent can be relied on as basis under common law.

All organisations that are covered by this Act will therefore have to ensure the mechanisms are in place to comply with this duty and helps support the notion that explicit consent is not needed for such sharing when providing integrated care (assuming the condition of implied consent are met). This duty only applies to adult social care data.

National Data Guardian

In her role as National Data Guardian, Dame Fiona Caldicott released a report in December 2017[14] outlining the three guiding principles of the use of patient/service user data. The first principle relates to the use of sharing for of information in the interests of providing direct care to an individual, which states:

There is a responsibility on clinicians and other members of the care team to share information that directly affects the care of the person they are treating or supporting. Patients and service users expect this, and my interventions will focus on supporting and reinforcing this approach. The direct benefits such sharing can bring to people, by providing joined-up care, better diagnosis and treatment, are unquestionable

The report recognises uncertainty from professionals about when implied consent can be relied upon to share confidential information and the National Data Guardian Panel are currently undertaking work to look into patient/service users understanding of what and when they would expect information be shared about them.

This being said, the report does note that *'Implied consent is a legal basis in common law. It is relied upon by health and care professionals every day to ensure good care is informed by the right information about an individual (although it should be noted that in social care settings it is common for people to be asked explicitly about what information may be shared).'*[15]

[12] Page 13, Confidentiality – guidance for registrants
[13] Section 251, Health and Social Care (Quality and Safety) Act 2015
[14] National Data Guardian for Health and Care 2017 report: Impact and influence for patients and service users
[15] Page 8, National Data Guardian for Health and Care 2017 report: Impact and influence for patients and service users

SWL Interoperability Solution

The SWL Interoperability Programme is designed to connect health and social care providers systems from across SWL to help facilitate the sharing of health and social care information for the purposes of direct care.

One of the key aspects identified in the Data Protection Impact Assessment for the programme was ensuring a defined process to enable lawful sharing and allowing patients/service users to opt-out of their confidential information being viewable via the Cerner HIE platform.

Data Protection

It is proposed that the lawful basis for processing will continue to be medical purposes as described above, with the availability of vital interests when required. This will continue with the introduction of GDPR.

Common Law

The two integrated systems in SWL, the Kingston Care Record and Sutton Integrated Digital Care Record, currently work on an explicit consent model to meet the common law duty of confidence. In practice, this means that every time the record is attempted to be viewed, a message appears asking the viewer whether they've asked for the patient/service user's explicit consent, or if this can't be achieved, a reason entered as to why this is (such as patient incapacitated). Figures from Cerner show that in one London Trust, explicit consent was not gained in 39% of the times the record was accessed. Whilst it is likely that a number of these patients would have been unable to provide consent, it questions how many times clinicians were accessing the record not in line with the consent model that was being relied upon.

It is proposed to move to an implied consent model for the new interoperability solution to meet the common law requirements, which could be implemented in two options below. This is in line with other models being proposed and revisited across London and England.

Meeting Requirements of Implied Consent in Common Law

If an implied consent model is chosen, the requirements described above will have to be met. This section will provide assurance on how each will be met and documented.

Use for Direct Care

The interoperability programme is designed to share information between providers for the purposes of direct care. The Information Sharing Agreement between the organisations will reflect this and put an onus on organisations to ensure their staff are aware of this. Any use of this information for non-direct care purposes without a lawful basis will be considered as a breach of the Data Protection Act and/or common law duty of confidence.

Fair Processing

Informing patient/service users of the sharing is a fundamental requirement of both privacy and confidentially laws. It also forms a right of the NHS Constitution, in that 'You have the right to be informed about how your information is used'.

Principle 1 of the Data Protection Act 1998 requires that processing is fair, in that data subjects have information made available to them about the processing. This requirement is further strengthened in GDPR, with Articles 13 and 14 listing a number of requirements that data subjects must be made aware of, depending on where the personal data is coming from. As seen above, to be able to rely on implied consent for sharing personal data for direct care to meet common law requirements, patient/service users must have information made available to them about such

sharing, and how they can object to such sharing. This can be summed up as ensuring there are 'no surprises' to patient/service users about how their personal data is shared.

As part of the Interoperability Programme information governance work plan a paper has been written on the fair processing campaign. This details the information that needs to be conveyed to patient/service users and the various methods of how this can be achieved.

Objection and Opt-Out

Both privacy laws and confidentiality laws provide the right to object to processing. Whilst this is not an absolute right in either case, it should always be taken into consideration when making a decision to share information. This is evidenced by both the GMC guidance and the 2013 Caldicott Report, and the Duty to Share does not apply where a patient/service user has objected or would be likely to.

GDPR provides a right to object where the processing is based on the public task lawful basis. In such cases the processing must cease unless the data controller can demonstrate *'compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.'*[16]

Common law provides that implied consent can only be relied upon when there is no reason to believe the patient / service user has objected, so it follows that there must therefore be a way to dissent to such sharing.

The SWL Interoperability solution will allow for patient/service users to opt-out of allowing their records to be viewed across providers via the Cerner HIE. In such cases, records will have to be requested and sent across to providers in more conventional methods each time there is a new episode of care. Whilst this opt-out will stop providers being able to access patient/service user records through the interoperability solution, it will not automatically stop any sharing of data for purposes other than direct care where there is a legitimate lawful basis to so, such as safeguarding concerns. The fair processing campaign will make this clear to the public.

Patients/service users will be able to opt-out of the sharing with the completion of a form which will be available on every participating organisations website. This form will detail the clinical risks of opting out and be accompanied by an FAQ's on the likely concerns and queries patients/service users may have around the solution. In other London areas this opt-out process is accompanied with a call from a clinician to discuss the decision with the patient to confirm they still want to go ahead given the potential consequences. This is something that could be considered for SWL.

Whilst the system may have capability to allow patients/service user to block specific organisations from viewing records, it is suggested that due to the infancy of the interoperability solution in SWL that the opt-out is restricted to a share with all or none model. It is planned that the system will in the near future link into the Healthy London Partnership's Health Information Exchange which is proposed to have a 'Patient Portal' which will allow patients to decide their sharing preferences about which organisations can see their data. This will then link directly with the national opt-out programme. This system should allow for the local opt-out form process to become redundant and take the management of this away from the organisations to the patient/service users themselves. It is proposed that only when the system is more advanced will patients/service users have the ability to pick and choose the organisations to share with.

[16] General Data Protection Regulation, Article 21

Duty of Confidence

The requirement for staff to have a duty of confidence is also found in the conditions for using the medical purposes lawful basis in privacy law[17]. Staff accessing the personal data to use for direct care will have a duty of confidence through their respective registered medical profession or their employment contract. Each provider organisation will already have systems in place to ensure that only staff with a lawful basis to access personal data can so. Maintenance of these will continue to be the responsibility of each individual organisation.

Role based access controls will be an important element at local level and form part of the requirements of signing the information sharing agreement. Organisations will ensure that clinicians will only be able to access parts of a patient/service user record they need to see in order to provide care to the patient.

Liability

A large concern around sharing health and social care data is the potential consequences of unlawful sharing. It was requested at the January 2018 SWL IG Working Group for this paper to include details of how organisations could become liable in the case of a breach of confidentiality or privacy law. This can be broken down into two areas.

This is guidance only. All incidents should be treated on a case by case basis. Legal advice should be sought by organisations that require further information.

Unlawful access

By staff

Unlawful access, where a record is viewed with no valid legal reason, normally maliciously, is an offence under both common law and data protection laws. In 2017 the Information Commissioners Office prosecuted eight NHS employees for unlawfully accessing personal data with no lawful basis. In these scenarios, whilst the ICO look at internal issues such as training and role based access controls (which should be at the core of data sharing even at local level), it is the individuals themselves that were liable.

For purposes other than direct care

The interoperability solution is to be used for direct care purposes. If information was pulled off for other purposes, such as research, without informing patients and having a sufficient lawful basis this would be considered a breach of both data protection and common law. The organisation responsible for this would be considered liable.

A caveat to this would be if there was a lawful basis which meant that patients did not need to be informed. Examples of this would be disclosures necessary for the prevention and detection of crime. The fair processing notices will make clear, however, that this could be the case and that no guarantee can be provided that information will never be shared.

Unlawful disclosure

Unlawful clinical disclosure

Another cause of complaint could be the allowance of personal data to be accessed via clinicians at other organisations. The risk of this complaint is likely to be directly related to the information available to patients about the sharing.

[17] General Data Protection Regulation, Article 9(3)

Clinicians will only be accessing personal data for the purposes of direct care (any other purpose would be covered in the unlawful access above). If a complaint was made that a clinician had accessed personal data of a patient for the purposes of direct care, which the patient was not aware of, a complaint could be made against both the organisation viewing the data and the data controller of the original data. The defence of such a complaint would be based on the safeguards of the system and the evidence of information already provided to the public about the sharing of data. This comes back to ensuring there are no surprises about the sharing of personal data.

Unlawful disclosure of confidential information

Certain types of information have an extra level of expected confidence, and in some cases have specific laws around disclosure. If the system is not able to exclude data from being shared, and this information is disclosed, a complaint could follow against the data controller of this information. Such information is being identified in the Data Protection Impact Assessment to ensure this is handled before the start of any sharing.

Options

Option A – Explicit Consent to meet common law (Current)

This option would see the current system remain, so each time an individual tried to access a record a message would appear asking the individual whether the patient has consented to that single access.

Pros:

- Would ensure the patient is made fully aware of the access
- Would provide evidence of consent in the event a complaint was made

Cons:

- Explicit consent is not required to access records for direct care where certain conditions are met
- Adds another level of process before direct care can be provided
- The conditions required to meet consent in common law following Montgomery vs Lanarkshire Health Board[18] could be difficult to meet each time a record is accessed and prove compliance with such conditions.
- Issues of how long consent lasts and whether it's for the episode of care or each time the record is accessed (e.g. can a doctor access a record before seeing the patient, or have to wait until the patient is in front of them)
- Could cause confusion for patients (and staff) as to whether explicit consent is also GDPR basis for processing. Consent under GDPR provides more rights to patients and has widely been reported to not be suitable for processing by public bodies.
- Doesn't follow the direction of other London STP areas which could cause issues later down the line when (a) agreeing a London wide model and London wide Data Sharing Agreement

Option B – Implied consent to meet common law

This option removes any prompt on the system and relies on the fair processing notices and opt-out availability to allow clinicians and staff with duty of confidence to access the records for direct care.

Pros:

- Allows clinicians and staff with duty of confidence to access patient/service users records whenever required for direct care purposes only

[18] Montgomery v Lanarkshire Health Board [2015] SC 11 [2015] 1 AC 1430

- Ensures patients/service users only receive information from the fair processing campaign so the message is always consistent
- Following patterns of other similar interoperability projects throughout London and England
- Supported by various regulators and national guidance

Cons

- If fair processing is not sufficient then complaints could be made against the sharing of information

Outcome

This paper is to help inform the discussion surrounding the model to be used for the interoperability project. The recommended option is option B – rely on implied consent to meet the common law duty of confidence. The requirements to use implied consent for direct care have been documented along with how the SWL Health and Care Partnership (HCP) is working to ensure these are met. Going with this option will also align SWL to other HCP areas which are moving towards implied consent models, as well as a London wide model which is likely to be implied consent based on the majority of HCP area's taking this approach.

The IG Working Group is asked to review this paper with a view to a decision being made at the March SWL IG Working Group.

Joe Stock
Information Governance SME, NELCSU