1 St George's Road,
London SW19 4DR

T +44 (0)20 8780 2211
F +44 (0)20 8780 1141
DX 300118 – Wimbledon Central

www.capsticks.com

Zoli Zambo
ECI and Digital Programme Lead
South West London Health and Care Partnership

11th September 2018

Your ref:
Our ref: **CYR1/128416**/21527322

Your contact:
Andrew Latham
T 020 8780 464
E Andrew.latham@capsticks.com

By Email Only

Dear Zoli

INFORMATION SHARING - SOUTH WEST LONDON

You have asked us to prepare a short note on liability and risk issues associated with the proposed data sharing programme in South West London. We understand that:

- The data sharing programme is a 'read only' arrangement, whereby different providers will be able to see recent records from other providers that are part of the scheme;
- The scheme follows the successful approach taken in South East London;
- The use of the data would only be for direct care.

Our understanding is that there is a particular concern from some providers that a 'rogue' member of staff at one organisation may pull up access to and misuse the combined records of a patient from other providers, which would expose those original providers to the prospect of a claim.

Our views on risk

In our view, the relative risks associated with the proposed arrangements are quite limited. The proposed use of the scheme is for direct care. S. 251B of the Health and Social Care Act 2012 imposes a duty on 'relevant persons' (commissioners and providers of health and social care services) to share information about a patient or service user with any other relevant providers or commissioners with which the relevant person communicates about that patient or service, to support the care and treatment of the individual user unless the patient objects. We understand that the SWL service is for direct care and so in our view the use of (explicit) consent is legally unnecessary and the statutory presumption is that sharing should take place. This is also reflected in the

seventh Caldicott Principle, which states that the duty to share information can be as important as the duty to 'preserve confidentiality'. Providers should be mindful that refusing to engage in the programme may carry a reputational risk, because patients will increasingly expect their data to be available between services.

GDPR

We are also satisfied that the sharing of information meets a relevant 'legitimising condition' for the purposes of Article 6 GDPR, namely:

> 6(1)(e):*"Processing is necessary for the **performance of a task carried out in the public interest** or in the **exercise of official authority** vested in the Data Controller".*

The Data Protection Act 2018 ("DPA") section 7(1)(a) defines a public authority as including "*a public authority as defined in the Freedom of Information Act 2000)*". Most health or care bodies (including GP practices) are a 'public authority' under Schedule 1, of the Freedom of Information Act 2000, and are therefore 'public authorities' for the purposes of the GDPR when performing a task carried out in the public interest (i.e. the provision of health or care services) or in the exercise of official authority vest in it.

Section 8 of the DPA states that processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority including processing of personal data that is necessary for (including) *"the exercise of a function conferred on a person by an enactment or rule of law"*. Health and adult social care providers are subject to the statutory duty to share information about a patient for their direct care pursuant to section 251B of the Health and Social Care Act 2012.

In our view the programme of work in SWL therefore meets the criteria for, and can rely on Article 6(1)(e) for processing direct care data. This is consistent with the NHS IGA guidance which covers the legal basis for processing personal data.[1]

We also consider Article 6(1)(c) may be an appropriate alternative basis for processing:

> "6(c) the processing is necessary for compliance with a **legal obligation** to which the Data Controller is subject".

[1] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance

An organisation can rely on this lawful basis when it is obliged to process the personal data to comply with the law. Again, section 251B of the Health and Social Care Act 2012 creates such an obligation to share information for direct care purposes.

Special Category Condition for Processing

Special Category Personal Data (SCPD) is defined as *"Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".* Processing SCPD is prohibited unless one of the conditions in Article 9 GDPR applies.

Article 9(2) of the GDPR sets out the conditions for processing special category data. Again, consent is a condition for the processing of special category data (pursuant to Article 9(2)(a). However, the most appropriate Article 9 condition for processing SCPD in the delivery direct care is Article 9(2)(h) which states:

> Processing is necessary for the purposes of 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 Data subject State law or pursuant to contract with a health professional.

Schedule 1 paragraph 2 of the DPA makes clear that SCPD can be processed if:

> *(1) …. the processing is necessary for health or social care purposes.*
>
> *(2) In this paragraph "health or social care purposes" means the purposes of—*
>
> *(a) preventive or occupational medicine,*
> *(b) the assessment of the working capacity of an employee,*
> *(c) medical diagnosis,*
> *(d) the provision of health care or treatment,*
> *(e) the provision of social care, or*
> *(f) the management of health care systems or services or social care systems or services.*

This is consistent with the NHS IGA guidance as well as ICO guidance, and therefore there is no GDPR impediment to data sharing under the proposed scheme.

Rogue employees

There is always a prospect of a rogue employee and the legal direction of travel (following the decision in *Various Claimants v Morrisons)* is that the employer will be responsible ("vicariously liable") for the actions of a rogue employee. However, that risk is already present in relation to the staff/records held by each organisation at the moment, and we do not think that the fact that there is the prospect of pulling up a view of recent records across multiple providers materially increases the prospect of an employee 'going rogue'. It would be would be helpful to understand from colleagues in South East London what, if any, incidents have occurred in relation to the information. We take the view that in practical terms, it is much more likely that an individual whose data is misused would bring a claim against the organisation that was (directly/obviously) responsible for the employee/incident, rather than the organisation that originally and lawfully provided the information. In other words, if the employee of organisation *X* misused data provided by organisation *Y* as part of the scheme*,* we believe the claim would likely be brought against organisation X rather than Y.

Article 82(3) GDPR provides that where there are multiple data controllers involved in an incident and some of them are "not in any way responsible for the event giving rise to the damage", they bear no responsibility. The level of culpability held by a party that was not directly involved in a breach, but was involved in a legitimate information sharing exercise, should, in our view, be considered minimal. Further solace is given in the recent European Court of Justice judgment in *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (the Facebook fan-page case), where the Court held that *"the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."* Additionally under Article 82(5) GDPR, where a claim is brought against one (responsible) data controller, it is possible for it to recover the costs/damages from the other (responsible) data controllers.

There are various other ways to manage or mitigate risk:

1) Clear delineation of risk within the information sharing agreements associated with the project. We are adopting a line that the organisation (directly) responsible for the breach clearly acknowledges that they will indemnify the others if claims are brought against them;
2) Robust and agreed arrangements/common standards and expectations around role-based access, audit logs, etc. and other technical measures to minimise the opportunity for misuse of the shared data;
3) Staff training and messaging to remind individuals that they should not misuse the data in question, and the potential consequences of misuse;

4) Strong public engagement prior to the project going live – this should help to ‘flush out’ those individuals who may be actively opposed to the information sharing exercise, minimising the prospect that their data falls prey to a problem.

The above measures can be worked into the project documentation.

Next steps

I hope the above is useful. If you have any questions at this stage please do not hesitate to let us know.

Yours sincerely

Andrew Latham