Video 2: Using and Sharing Data for Casework

Welcome to video two in this in this series of bite-size e-learning modules on good data collection, storage and use in frontline services. In video one we talked about good practice and some legal considerations when it comes to collecting and storing information or data about the clients you are working with. In this video we will look at using and sharing the data you hold about anyone your service is currently working with or has supported in the past.

Using client information

Once you have collected information directly from your client, or about then from a third-party source, you will want to use it in order to get the best possible outcome for them. You might also want to share it with other organisations, for example in referral forms to accommodation and other support services, or during multi-agency meetings such as casework panels or regularly held rough sleeper or homeless action group. In this video we will look at good practice and some further legal considerations you need to be aware of when you are using and sharing client data in your day-to-day work.

In video one, we talked about the need for a lawful basis for collecting information from those you are working to support and looked at some examples of lawful basis. If you haven't watched video one yet, pause here and watch that video before carrying on with video two.

Sharing Client Information

You also need to have a lawful basis for using and sharing the information you hold about a client when carrying out your role. In such instances sharing will often be on the lawful basis of consent or public task.

If you are sharing information with other teams or services on the basis of consent, as mentioned in video one, it is important that you take measures to ensure that client consent is informed and recorded, for example it is written rather than verbal. But you also need to ensure that consent is on-going. For example, you might tell a client you have been working with for a number of days or weeks that you would like to refer them to a particular project or service. If a client tells you, for whatever reason, they don't want their information to be shared with that organisation they are withdrawing consent, meaning you no

longer have that lawful basis for sharing it in this instance, even if your client has previously signed a written consent form.

This is why it is important to always be transparent with clients about when and how information about them will be shared and discussed, and why it is important to ask before sharing. It is a way of not only ensuring on-going consent but also of earning trust.

Data Sharing Policy

Most organisations have a data sharing policy, and where organisations regularly work in partnership with other organisations they will often have a specific data sharing agreement in place. What data sharing policies and protocols does your organisation have in place? Do you have an information security officer whose role it is to ensure information is collected, used and stored by the organisation in a lawful way? If you're not sure, check your organisations policies and procedures, and if you can't find one, ask your line manager.

Even once you establish a lawful basis for sharing client information, you must only share what is necessary for the task at hand. What this means, for example, is if you are discussing someone you are working to support at a multiagency, meeting with the hopes of securing them a supported housing placement, is it relevant and necessary to talk about adverse childhood experiences they might have disclosed to you? If there are certain situations that risk triggering a trauma response in your client, it may be appropriate to talk about that. But, while it might feel relevant, it is not always necessary to divulge the details of the traumatic experiences.

Another example might be if you are working with someone who has fled domestic violence and describes to you some of the violence they were subjected to. When referring to a specialist domestic violence service, it might be relevant and necessary to provide some of these details. However, when making a referral to a drug or alcohol support service, it might only be necessary to share that your client has been a victim of domestic violence to ensure they are able to access single-gender support, for example, but the specifics of the abuse that your client has suffered are not relevant and don't need to be shared.

Accessing Information Unnecessarily

Another important principle of good data use, which is often overlooked, is that you should never access information unnecessarily. For example, having a login to your organisation's client casework database doesn't mean it's appropriate for you to look up information about individuals you've never worked with, or anyone who you've worked with in the past. It's easy to wonder how former clients are getting on and to be tempted to look for any updates on databases or client files we have access to. However, as this is not a requirement of your role or necessary to carry out casework it is inappropriate and could contravene your organisations data protection policy.

Sharing Logins

Similarly, you must never share any of your database or other systems logins with anyone for them to be able to access information about clients. If someone needs to access client casework files or databases, they will be provided with a login by your organisation. If they don't have one, they should not be accessing those files.

Sharing Client Information with Statutory Authorities

A question that often comes up is what, if any information is it appropriate to share with statutory services?

The short answer is, the police have no right to demand you to share information about clients, their history, their whereabouts and so on, unless:

- They produce a warrant for this information
- The police legitimately believe that the client in question is about to, or is in the process of committing a serious crime or is the victim of crime.

In both cases, this does not mean the police have the right to any and all information you hold about the client. A warrant will stipulate what information the police have been asked to search for. Or, in an emergency situation, the police only have a right to access information that will help to prevent a serious crime being committed, locate a victim or apprehend a perpetrator.

The UK Immigration Enforcement service does not have the same powers as the police to access information about people you are working with. You are under no legal obligation to disclose information to them.

If you are asked by the police or any statutory body to provide information, it is strongly recommended that wherever possible you escalate the request to your service manager, or information security officer if your organisation has one.

Personal Data Breach

Your clients have legal rights when it comes to having their personal and sensitive information protected, and organisations and their workers have legal responsibilities. If personal information about anyone you're working with is stored, shared or accessed inappropriately, this could be what's known as a personal data breach, which is defined by the Information Commissioner's Office as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data' and which is likely to result in a risk to the rights and freedoms of the data subject.

This could be something as simple as a notebook containing information about clients being left on the bus, or an email with a completed referral form attached to it being sent to the incorrect recipient.

If a personal data breach does take place, you must report it to a team leader or service manager, who will then need to arrange reporting the data breach to the ICO. In larger organisations with an information security officer, they will usually make the report. In smaller organisations, it may be the CEO or a director who is responsible for making the report. Whatever the case may be, by law the ICO must be notified, and where required an official personal data breach report submitted, within 72 hours.

Suggested activities

In a team meeting, discuss;

- the different organisations your service shares client information with, why and how
- whether what has been covered in this video has made you think differently about sharing this information
- the process (internally) for team members to report a personal data breach,
- the process (internally) for responding to requests from the police for information about clients
- the process for responding to requests for client information from any other outside organisation or statutory body,
- whether these processes are included in new starter induction training

Suggested actions

- Find out whether your organisation has a data sharing policy and if so, share it with your colleagues. If not, find out from your service manager how your organisation can go about drafting a data sharing policy.