Hello, Karen from Gravitas Outcome Services CIC here!

I want to talk to today about the basic principles relating to storing a person's information, and the appropriate protection and sharing of this. It is not intended to be an authoritative account of the legislation as it applies to you, in either your country or organisation. Indeed unless you have all day, or maybe even all week, it would be impossible to do this within the scope of a short podcast such as this. It is more intended as a discussion topic that should encourage you to think about your position and how the rules around data gathering may affect you. I have listed a number of more authoritative links on the webpage should you want to explore this topic further. It will be necessary for you to consider all that I say within the policies already set out where you work, or legislation in the country that relates to you.

It is important to distinguish here that I am not necessarily just referring to data that is stored electronically, such as in CORS. I have been witness throughout my working life, sadly, to some very poor practise with regard to protecting information about clients generally. The most significant of these that comes to mind is the commonly used 'signing out board'. These are often found in social care settings, where workers are out of the office visiting clients in their home. They can neglectfully identify service users to cleaners, caretakers and anyone else who happens to have access to the building out of office hours. In this way, we can see that data protection is not always restricted to sci-fi style big brother is watching you.

Firstly, let's think about why we should be recording and sharing data at all. You may need to have contact details of a client so that you can advise them of upcoming events and activities, or pass on useful information to them. If you are working with a client on a longer term goal you may want to chart their progress along a path. All of these aspects are of benefit to the service user, and as such are unlikely to raise general concern. I'm sure you can think of a lot more reasons why having some records about the person that you work with help you to do a better job.

Historically, as computer use for storing information became more widespread, and news stories of hacking etc. became part of mainstream media, concerns grew about what information was being stored and the safety of this not being shared inappropriately. Indeed there have been many instances of sharing that have caused direct harm, such as when test results for HIV Aids were shared with health insurance firms, leading to an increase in premiums. These matters still cause great concern, and the subject is becoming ever more relevant with threats of terrorism and exposure of telephone monitoring records being leaked.

The key factor then, is where to find a balance between data security and useful storing and sharing, in order to improve the efficiency and effectiveness of services whilst respecting a person's privacy. In the late 1990's the government ordered a review of data gathering in health and social care settings which was undertaken by the Caldicott committee. The findings recommended applying 7 general principles to data gathering and sharing.

Ask yourself if you think they are satisfactorily implemented by you in your organisation, we will go through them in turn:

1. **Justify the purpose:**

   Do you understand why you are gathering data, if not, could you ask a colleague? If they don't know, then maybe your management team could help. If you are management, then maybe a review of what you are collecting and why, is overdue. Be clear, and specific, too often I see organisations just going through the motions because they know they need to record something!

2. **Don't use personal confidential data unless it is absolutely necessary:**

   Many of our organisations use unique identifiers such as a membership number or nickname, or when they have large changing groups of service users just anonymous 1,2,3,4 etc... In this way, they get to count data, but it cannot be related back to a person. This may not be helpful when you really do want to ensure that you are dealing with a client in a personal manner, or charting. Again, we are trying to find the right balance.

3. **Use the minimum necessary personal confidential data**:

   Some of our services find it really useful to record every detail, others find that just attendances will do. This is why CORS is so flexible in what you have to record, you can keep it minimal, or record every detail. Again, refer back to your purpose!

4. **Access to personal confidential data should be on a strict need-to-know basis:**

   Many of our services use volunteers for some aspects of data gathering, and we are aware that it would help if there were separate levels of security allowing access to only necessary information. This is something we are working on. We have started to change the forms so that comment fields have to be clicked on to see them. This is where we will introduce levels of access together with membership groups, so that services can allow more people to interact with CORS in the future.

5. **Everyone with access to personal confidential data should be aware of their responsibilities:**

   This is something only your organisation can answer, training should happen, do you know your responsibilities? If not, ask your managers!

6. **Comply with the law: Every use of personal confidential data must be lawful:**

Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements. Do you know who your data controller is? They are responsible for ensuring the data you collect meets with this requirement. I have linked a couple of sites that outline the Data Protection Act of 1998 as updated in 2003 for you to look at too.

7. **The duty to share information can be as important as the duty to protect patient confidentiality:**

   Can you think of instances where you should share information? What about if somebody has shared something with you that might identify a risk of harm to themselves or others? What if you could help to improve somebody's situation by sharing information with another organisation? Do you have that person's permission? Should you gain it? Do they know what information you hold, and have they agreed to this?

There are major considerations associated with the above that require some concentrated effort of time and thought. It is important that you can be open with your clients about what you are recording and why, and that this also requires constant review. Remember they have a right to see any information you hold about them, avoid discriminatory language, and ensure you have appropriate evidence to support your records.

The main data protection legislation pertaining to our services in the UK at the moment is the Data Protection Act of 1998, amended in 2003. As I said before, I won't give a full account of this legislation, but you can find it again in a link on this page. I would however draw your attention to the 8 basic data protection principles, some of which overlap with the Caldicott findings so I won't repeat them here, but will add where necessary. I have highlighted the difference between personal data and sensitive data in the document link on this web page. Please take some time to consider this in relation to the 1st principle as they apply differently in this case.

The Eight Data Protection Principles

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, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall not be further processed in any manner incompatible with the original purposes.

Essentially, this means that you should not use your data to sell elsewhere for instance as a marketing tool maybe, importantly if you stick to your original purpose you should be fine.

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.

   We take this very seriously, and hope that you will always let us know IMMEDIATELY if you have any concerns about a loss of data, or incorrect storage.

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

6. Personal data shall be processed in accordance with the rights of 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. You should know that all CORS data is held in one of two places, either in Holland or Ireland.

This brings me to one final point. There is currently in force a new EU directive that looks at data protection and sharing. I have chosen not to cover this in detail, mainly because it will not become part of law until 2018, but also because of the issues of Brexit, it may not even be implemented in its' current form. Importantly however, it is more to do with the kinds of data collection that happens in between businesses coincidentally for instance, when you use a credit card online or in a store, this information is often shared to target marketing approaches. If you are adhering to current legislation principles whereby the data is only being stored for the purpose of improving your service, and not processed in any manner incompatible with that, you should be fine. There is also a link on this page however should you like to investigate this further.

I hope this has been helpful, and that you find the time to explore this topic further using the links I have provided. Please do not hesitate to get in touch if you would like to ask further questions.