An Introduction to Information Sharing for Staff

1. What is Information Sharing?

Information Sharing is the way organisations safely share, process and handle personal information (e.g. service user & staff files) and business information (e.g. financial records & contracts). The methods used to keep this information safe are called Information Governance.

The protection of sensitive and confidential information is both a legal requirement and a contractual obligation. Protecting information is a shared responsibility between you and everyone who works with you, not just your manager or senior staff team.

2. What does this mean for me?

Information sharing rules must be followed to ensure that service users and staff are confident that their information is: safe, accurate, and only available to those who need it! Knowing how to safely share information helps your organisation and helps you!

This guide will tell you about the different types of information you might come across in the course of your work and how you can ensure that it is always shared appropriately.

As part of your job you are required to:

1. Know how to safely and appropriately share information.
2. Follow procedures to make sure that sensitive and confidential information is properly protected. Failure to follow these procedures may result in disciplinary action.
3. Immediately report to your line manager any information security breaches. If you are unsure if it is a breach, it is better to ask.

If you feel you need more training on Information Sharing, please speak to your line manager who will make the necessary arrangements.

3. What kind of information must be kept confidential?

In your job, you might have access to lots of different types of confidential information such as: medical records, payroll details, the kind of car someone drives, staff sickness, if someone has a criminal record, personal information and many others!

You can gain access to this information in lots of ways: through email, fax, computer files, paper records, and even through a conversation – either on the phone or in person.

4. How can you keep information safe?

There are a number of things you can do to make sure that you keep information safe.

These include:

Physical Measures

- Remember to lock rooms which contain confidential information when they are empty
- Use tracked post to ensure that it reaches the correct person.

People Measures

- Confidentiality & security training – if you feel you need more training on these topics, you need to speak to your line manager.
- Identity Checks – always make sure you know who is asking for information and why
- Report any security breaches to your line manager.
- Portable devices – if you have access to a mobile phone, laptop or tablet, follow your organisation's policies on the safe use of these devices; https://www.getsafeonline.org/smartphones-tablets/

Electronic Measures

- Strong passwords – use 3 random words to easily make a strong password; https://www.cyberaware.gov.uk/passwords
- Locking Computers When Not in Use (press the Windows Key + L)
- Secure Email – be careful when clicking on links and attachments and always delete scam and spam emails; https://www.getsafeonline.org/protecting-yourself/spam-and-scam-email/
- If you use computers in your organisation it is vital that you are aware of the importance of cyber security. Further advice can be found: https://www.cyberaware.gov.uk/.

Ask yourself whose information you are using and who should have access to it. If you are not sure if someone should see the information, it is better to clarify with your line manager.

5. Information Sharing and Consent

The consent of citizens is fundamental, not only to their care but also to the information that we keep and share. It is important that our service users know and understand how their information is being stored and used and who has access to it.

All service users have the right to be involved in the preparation, review and continued management of their care plans and should know how their health records will be made available to them.

Information should only be shared where necessary and/or with the consent of the service user.

Many service users will be happy for their information to be shared for the purposes of their care *e.g.* with Doctors and Nurses, but may not be content to have their information shared for other purposes. You should ask yourself why you are sharing the information.

If you are a carer, does the receptionist need to know the details of someone's illness?

If you work in reception, should you be telling people why a member of staff is off sick?

It is important to ensure that confidential and sensitive information is kept safe, but this should not be a barrier to sharing information.

6. Case Studies

Case Study 1

You overhear two other members of staff talking about a resident in the supermarket. What should you do?

a) Join in. They may have information you need to know.

b) Go to your line manager and ask for them to be fired.

c) Speak to them and say that this behaviour breaches confidentiality.

Case Study 2

You see that another member of staff has forgotten to lock their computer and it is showing a service user's health record. This is not the first time. What should you do?

a) Use the computer to send some e-mails

b) Nothing. They will only be a moment

c) Lock the computer for them and report them to your line manager.

Case Study 3

You notice that a fax has arrived on the fax machine with hospital discharge papers; the fax machine is in a public area. What should you do?

a) Turn the papers upside down so that no one can see them

b) Hand over the papers to your line manager and report the incident to them

c) Read the papers to see who they are talking about

Case Study 4

You see a service user you know socially in A&E and you phone a mutual friend to let them know. Is this OK?

a) No, this is confidential information

b) Yes, the mutual friend would like to know

c) Yes, because my friend in A&E may like the support.

Answers

1. **The correct answer is (c).**

   If you overheard them talking, then so could anyone else. If you feel it is appropriate, this might be something you wish to raise with your line manager, especially if it happens repeatedly.

2. **The correct response is (c).**

   The computer is displaying confidential information which could be a serious information security breach. You can quickly lock the computer by pressing the Windows Key + L. You should raise this with your line manager so that they can take corrective action to ensure that everyone has received training on confidentiality and so that they are aware that there could have been an incident.

3. **The correct response is (b).**

   Hospital discharge papers contain confidential information which should not be left out in public spaces. Handing them to your line manager and reporting the incident means that they can take steps to ensure that this potential breach of confidentiality does not re-occur.

4. **The correct response is (a).**

   Even though it is tempting, the service user's presence in A&E is confidential information and disclosing this – even to a mutual friend! – could cause upset and distress.