NHS

Urgent Care 24

**T.H.E. I.G. C.O.D.E.** is a useful acronym to remind us what is expected of us in our day-to-day work. Each letter stands for a prompt that we should consider.

**Think** - when using personal information
**Handle** - information securely
**Encrypt** - all laptops, and memory sticks
**Information** – if it's personal, it's private
**Governance** – you are accountable for personal information
**Confidential** – prevent unauthorised disclosure
**Overheard** - remember: sound travels!
**Do not** - share passwords or smartcard PIN numbers - ever!
**Everyone** – we all have a legal duty to keep personal information safe and secure.

**Think**
Positive patient outcomes rely on us sharing information with our colleagues. However, we do need to think when to share, what to share and how to share. Consider the following:

- Can the person be identified?
- What is the purpose for sharing the information and is it appropriate to share?
- Does the information need to identify the individual or organisation involved or can it be anonymised?
- How should it be shared – are you storing and transferring the information securely?
- Are you or they authorised to have access to it?
- Have you told the patient – do you need their consent?

We all need to think carefully when we share information and make sure it's protected when we do. If you're unsure of whether you should be sharing, it's ok to ask. If you'd like more guidance around this speak to your Line Manager or your **IG lead**.

**Handle**
Handling information is part of our everyday job. Making sure it's being handled securely should be too. If the information falls into the wrong hands there could be damaging consequences for the patient, you, your team, the organisation you work for and the reputation of the NHS. To ensure confidential information is not unlawfully or inappropriately read, used or shared, ask yourself:

- Do you lock your screen when you leave your computer?
- Can others see the paperwork you've been working on?
- Do you leave paperwork unattended?
- Is the fax number you're faxing to correct and secure?
- If you're disposing of paperwork are you doing it safely?
- If you're deleting files is it being done securely?

Make sure the information you're handling is seen by the right person(s) only and shared because it is necessary for the health care and treatment of the patient or a business purpose of the organisation. If you're unsure of your responsibilities or are being asked to share information that you consider to be inappropriate speak to your line manager or your **IG Lead**.

**Encrypt**
The Department of Health policy says "Do not hold person identifiable data on portable media unless it is encrypted"
Encryption is a technical measure used to lock and protect information held on portable or removable media such as memory sticks, laptops, disks or mobile phones.

Patient, personal or organisation sensitive information must not be held on removable media, unless it is encrypted and in line with the Urgent Care 24 encryption policy. You should consider:

- If your laptop was to fall into the wrong hands confidential information could be viewed or accessed if it is not protected by encryption
- Is your memory stick encrypted?
- Do not share memory sticks with colleagues or even family members
- Do not upload and hold patient, personal or organisation sensitive information on non-Urgent Care 24 IT equipment ,

Urgent Care 24 has an encryption programme. Call the IT department if you need advice or help.

**Information**
If it's personal, it's private. Information can come in many forms:

- Emails
- Faxes
- Patient notes

- Telephone messages taken and left
- Conversations in waiting areas, between colleagues and on the telephone.

It is your responsibility to protect the privacy of personal information in whatever form you receive, hold or share it.

If you have been involved with or know of an incident involving a confidentiality breach or data loss you should always report it to your Line Manager or your IG lead. This will help us learn why incidents happen as well as develop ways of stopping similar incidents happening again. Ask your Line Manager if you are unsure. **IG Lead**

**Governance**

This is the management, policies and processes that we should all be using in our day-to-day work when handling patient, personal or organisation sensitive information. You have a responsibility to make sure that any information you hold and pass on is done safely and securely.

Your organisation will have its own Information Governance-related policies that tell you how to manage records, protect data and keep it secure.

- Do you know where to access them?
- When was the last time you read them?
- Have you had training on them?

To find out more visit the link to your organisation below.

https://extranet.urgentcare24.co.uk/logged_in.asp (you will find all policies and Sop's here)

**Confidential**

Sharing of confidential information is vitally important in many situations in the NHS. However, you should always think about the patients and colleagues you're sharing information with. The Data Protection Act and the NHS Constitution state there is a legally-binding right to keep confidential information safe and secure. Ask yourself:

- Is the person I am sharing information with authorised to see it?
- How much information do they need to do their job and should it be identifiable information ?
- Is it relevant to the purpose they need it for?
- How can I get it to them securely?
- Do I need to get patient consent to share it?
- Am I being sent confidential information when I don't need it?

If you have concerns or questions speak to your Line Manager or your **IG lead**.

**Overheard**
Remember: sound travels!  When we're in open spaces – reception areas, wards, corridors – or even if we're in an office with the door open others may overhear what we're saying.  Think about the conversations you have and the messages you leave:

- Can your telephone conversation be overheard?
- Is it appropriate to have that conversation in a public area?
- Can the patient you're talking about be identified by others overhearing?
- Are others listening to your chat with a colleague?
- Are you leaving messages that should not but can be accessed by others?
- Does your message need to identify the individual concerned?

You should think about the volume at which you're speaking and not be worried about telling others that you can hear them too.

**Don't share passwords**
If you've ever shared your password, Smartcard or PIN number consider:

- What if the person you've shared with has then shared your password with others? How many people potentially can access that information?
- Would you share your bank account and PIN number in the same way?
- What if something goes wrong as a result of a colleague using your password?  You will be held responsible – did you know it is unlawful and you are liable for that offence?

Passwords, Smartcards and PIN numbers have been provided to protect you and the information you have access to.

If you have shared your password or PIN number - change it now and take back control.  It may be necessary to inform colleagues you have changed it, but not what you've changed it to.

If others ask you to share your password or try to access a system when you are logged on, then you have a duty to challenge them.  If you have any concerns around sharing passwords then speak with your manager or your **IG Lead**.

**Everyone**
Everyone working for or with the NHS has a legal duty to protect personal information. You have a responsibility to keep personal information safe and secure.  Whether you're involved in transporting patient or personal files, maintaining databases or accessing patient or personal records you have to make sure it's done safely, securely and legally.  This applies to any personal information held in electronic and paper format.

If you have concerns or you feel you need more training you should speak with your Line Manager or your **IG lead**.