NHS
Gloucestershire Hospitals
NHS Foundation Trust

Simple guides

Information Governance

In this edition of Simple Guides we explore the issue of protecting confidential patient information.

All NHS employees are duty bound to uphold the principles of the Data Protection Act. This important legislation underpins how we are expected to behave with regard to managing confidential information. It is a key part of your employment contract with the Trust and is a requirement of clinical registration bodies, such as the Nursing Midwifery Council (NMC). The Trust must also satisfy its information regulator, the Information Commissioners Office (ICO), that we are managing patient information in an appropriate manner.

In this guide:

- Why is information governance important?
- How can we improve information governance day-to-day?
- What sort of situations should staff be mindful of?

Why is information governance important?

Maintaining a high degree of professionalism with regard to managing patient information is a vital component to the care we deliver.

Information must reach the right people so that effective clinical decisions can be made but information must also be protected from inappropriate access, so that patients can be assured and confident that their very personal details are not being misused.

If patients didn't have confidence in our ability to manage their information appropriately they would be less inclined to share their details with us, which could impact our ability to deliver the right care to them.

How can we improve information governance day-to-day?

Some basic understanding of the Data Protection Act is required to work at the Trust. This requirement is covered in your employment contract and is also covered in the Trust's induction session and in the annual mandatory training updates.

- Do not share patient information with anyone else unless they have a legitimate professional reason for needing to know.
- Minimise the amount of information you share, especially with third party organisations that aren't involved in the direct care of our patients. For example, if it isn't necessary to share the patient's name, don't. Just use the MRN number and date of birth.
- All staff should undertake their mandatory IG training which is available on the **intranet training pages**. This module is 15 minutes long and covers the basic IG knowledge you need as an employee of the Trust. This mandatory training should be retaken every year.
- It's important to be aware that the Trust has polices regarding how we manage information. You can find all you need on the intranet's **Information Governance pages**.
- Depending on your role, there are other organisations that will have an interest in your conduct. For example, if you are a nurse, the **Nursing Midwifery Council** (NMC) has Information Governance guidance and advice you should also be aware of.
- The Information Commissioners Office (ICO) is the overreaching regulator for the Trust. Their website is an excellent source of data protection guidance: **www.ico.org.uk**.
- As a general guide, it's helpful to treat other people's information as though it were your own. So ask yourself: if this was my information how would I feel about it being shared in this way?
- If in doubt, ask an experienced colleague or contact the information governance officer for the Trust. Contact: **ghn-tr.information.governance@nhs.net**
- If you become aware of an incident involving an information governance breach you should report the incident on the Trust incident reporting system. This system is called Datix and can be found on the intranet home page.

What sort of situations should staff be mindful of?

The organisation must protect the information we are entrusted with in order to function.

If we didn't do this, our patients and our regulators would soon lose faith in us. The Data Protection Act makes it clear that we must take all reasonable steps to ensure the information we manage is not accidently or deliberately compromised.

Confidential patient information is routinely used in a number of situations at the Trust and staff need to manage these situations appropriately as there is the potential for serious breaches of confidential patient information if the correct practice is not followed.

> "Information must reach the right people so that effective clinical decisions can be made but should only be shared for the purpose intended"

Taking confidential records off-site

Trust staff deal with very sensitive patient information day-to-day. It's easy to become relaxed about the data we are responsible for.

Patient information in physical records should only leave Trust premises if absolutely necessary. Do not take patient information off Trust premises out of habit.

Your workflow must support the Data Protection Act principles, so please consider the reputation of the organisation and your own obligations to uphold the Act.

If the management of patient information off Trust premises or between sites is necessary, follow these 'rules':

- Do not travel with confidential information on unprotected loose sheets of paper or use insecure means of storing it during transit. A secure sealed folder with no open sides or suitable strong case is recommended.
- Do not leave the information unattended at any point in your journey;
- Do not allow unauthorised persons to see the information (this includes other Trust staff who are not involved in the care of your patients);
- Do not travel with confidential information on public transport where possible;
- Return the information to Trust premises as soon as reasonably possible;
- All confidential information must be disposed of in confidential waste bins only.

Mobile phones and personal IT equipment

All staff have an obligation to ensure that electronic confidential data is not stored or transmitted insecurely.

It is not permissible to use unauthorised equipment to store confidential patient information. This includes the storing of patient identifiers such as names and NHS numbers.

The Trust provides a vast range of IT equipment for staff to do their work. All Trust owned equipment is encrypted, tagged and protected by a range of other security measures. Personal equipment is not protected to this extent and therefore the Trust cannot provide any assurance to our patients that these devices are secure.

It is therefore Trust policy to only use authorised equipment to store confidential data. If you want to use your own equipment to receive emails, you need to contact the IT helpdesk and they will advise you what is possible.

Emailing confidential information

There are many aspects of emailing confidential information to be wary of.

In particular, staff should be careful not to email patient information across insecure networks or to insecure email addresses without the express consent of a patient.

When emailing from a NHSmail email account to another NHSmail email address, the data is being transmitted within our network and is secure.

NHSmail accounts can be transferred between NHS organisations, so you can retain your NHSmail account even if you leave your employment with the Trust and go to work with another NHS organisation.

However, if you were to email a non-NHS organisation, or private email addresses, the data is moving out of our control and can be intercepted. Emailing patient identifiable data outside of the NHSmail system is therefore considered insecure, unless the appropriate guidance is followed and should not be done.

It is also advisable not to send emails to multiple recipients unless it is absolutely necessary, especially if private email addresses are involved. If you absolutely must send an email of this nature, ensure you understand the correct process to do this and have agreed this with your manager. You must 'blind copy' (referred to as 'Bcc…' in Outlook). If you don't do this, all the recipients will have the email address and therefore the contact details, of all other recipients.

Such circumstances can lead to serious breaches of Information Governance and have led to ICO investigations in other Trusts, most recently at a clinic in London.

Only send emails to multiple recipients if you absolutely must do so and you understand how to do this correctly.

Training

IG training is mandatory and must be done annually. Staff can access IG training on the intranet.

Follow the guidance on these pages to gain access to the essential training. Once you have gained access to your online training programme, you will be able to do your **IG eLearning** module.

The module is very short (15 mins). There is a short exam at the end of the module. Once you've passed this your training record will be updated automatically.

Accessing records appropriately

A fundamental aspect of the work of many staff at the Trust is the ability to access patient administration systems.

However, having the ability to access data does not give anyone the automatic right to see it.

Staff are only permitted to access records as a direct requirement of their role. Staff should only access patient data if they have a legitimate professional reason to do so. Staff should not access the records of a patient that they have no professional involvement with, nor should they access their own records, the records of family members, friends, partners, or anyone who is not under their care. IT systems are audited and all access can be retraced and investigated. If a member of staff is discovered to have accessed data inappropriately, they risk disciplinary action.

If you are performing administrative support to a team, then the same rule applies: you should only access records that you are required to as part of your role at the Trust. Being related to a person or knowing them personally does not give anyone the right to breach a patient's confidentiality.

Summary

- Do your mandatory information governance training on the Teaching and Learning portal.
- Ensure you have at least a basic understanding of the Data Protection Act.
- Ask an experienced colleague or contact the Trust's information governance officer if you are unsure what to do in respect of handling patient data.
- If you become aware of an information governance breach, you should report the incident on the Trust's incident reporting system, Datix.
- Only access information you have legitimate right to access.
- Ensure any emails that contain confidential data are secure.
- Do not use personal IT equipment to store or transmit confidential data.
- Be mindful when transporting confidential information that this information is private and should only be taken off site if absolutely necessary. Confidential information should be protected adequately at all times. If you absolutely must take sensitive information off site, ensure it is transported securely (eg use a sealed folder with closed sides).
- Limit email distribution to those who absolutely require the information undertake their role

For more information:

- To find out more about information governance, visit the Information Commissioners' Office website: **www.ico.org.uk**
- Additionally, there a number of useful pages on **our intranet**