- Confirm the identity of callers before giving out any sensitive information.
- Do not discuss patient-related issues in a public place.
- Under no circumstances should any paper records or laptops with person

Remember!

You must take all reasonable care to protect confidential information from loss, damage, unauthorized access or disclosure by:

- Keeping all person-identifiable information securely
- Not disclosing person-identifiable information to anyone inappropriately
- The loss or unauthorised disclosure of personal information (e.g. looking at data you are not entitled to) can lead to disciplinary action against the individuals concerned, or even prosecution in cases of malicious or willful misuse. It is important that any incidents or data breaches are reported on DATIX as soon as possible for an investigation to take place.
- We can avoid the number of data breaches reported by ensuring all staff are trained, please complete your annual information governance training.
- Do not post personal data on any social media sites.

Patients have the right to object to the use and disclosure of their personal information, and need to be made aware of this right. Informed consent must be obtained before personal data is used for any reason other than the patient's direct care.

Data subject rights

Under the Data Protection Act 2018, individuals have increased rights in relation to their information. These are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

If a patient, other staff member or member of the public contacts you about these, please refer them to the information governance department.

Contacts

For further information, please contact a member of the IG Team:

informationgovernance@eastamb.nhs.uk

Data Protection Officer: Emma Sears

NHS East of England Ambulance Service NHS Trust

Information Security & Data Protection

Protecting the Trust
Protecting you

Your legal duty of confidentiality

Everyone who works for EEAST is bound by the common law duty of confidentiality. This includes permanent and temporary staff, bank staff, contractors and volunteers.

You must treat all person-identifiable and sensitive information (clinical or non-clinical) as confidential. This applies to both patient and staff records.

You should read this leaflet in conjunction with the Trust's Confidentiality Code of Conduct, which is available in the **Document Library on East 24.**

What is person-identifiable and special category/sensitive information?

Person-identifiable information is enough information to identify a living individual. This might include:

- Name, address and postcode
- Date of birth
- Telephone numbers
- National insurance number
- NHS number
- Images such as a photograph

Sensitive information includes medical history, work performance, ethnicity, sexuality, political affiliation, religious beliefs and criminal records.

Where is this information held?

Confidential information could be held in many formats and media types, including:

- Medical records (PCRs)
- Personnel records
- Computer files and print-outs
- Laptops, CDs and memory sticks
- Faxes
- X-Rays and ECGs
- Voice mail and message pads

When you can share person-identifiable information

The Caldicott Principles stipulate that you can share person-identifiable data only if you:

- Can justify the purpose for using the information
- Use the information only if absolutely necessary
- Use the minimum information required for that purpose
- Ensure access to the information is on a strict 'need to know' basis
- Know that everyone who sees the information understands their responsibility to protect it
- Are you confident that recipients will comply with the law?

The duty to share information can be as important as the duty to protect confidentiality

If you are asked to share person-identifiable information and you cannot confirm all Caldicott Principles, you should seek guidance from your line manager, the Caldicott Guardian or a member of the IG Team (see contact on the back page).

Keeping information secure

- Be careful who you disclose information to. Do they really need to know? Can you justify the disclosure? Have you only given out the minimum data required?
- Never use anyone else's log-on ID or Smartcard or let them use yours.
- Do not send confidential information via a non-secure email provider (e.g. Hotmail). An nhs.net mail account must be used!
- Only Trust issued encrypted memory sticks should be used to store person-identifiable or sensitive information, with the prior approval of your line manager. Never transfer Trust data to your home computer!
- Keep paper records and mobile devices (such as toughbooks, laptops or USB sticks) physically secure at all times.
- Sensitive information in paper format (such as PCRs) must be kept secure at all times. Paper records should never be left in plain view in an open or public area.
- Ensure you log off when you finish using a Trust PC or laptop, and lock it when leaving it unattended.