## PERSONAL INFORMATION

The term 'personal information' refers to any information held about an individual (patients, relatives or staff) who can be identified from that information.

Everyone working for or with the NHS who comes into contact with information that could identify a patient or member of staff has a personal **common law duty of confidence** to those individuals and his/her employer (whether the information is clinical or not) This is written into your employment contracts.
Breach of confidentiality may lead to disciplinary action and could lead to dismissal.

## CALDICOTT PRINCIPLES

- **Principle 1** - Justify the purpose for using **patient** confidential information
- **Principle 2** - Only use it when absolutely necessary
- **Principle 3** - Use the minimum identifiable information required for that purpose
- **Principle 4** - Access should be on a strict need-to-know basis only
- **Principle 5** - Everyone must understand their responsibilities to protect information
- **Principle 6** - Everyone must understand and comply with the law
- **Principle 7** - The duty to share information can be as important as the duty to protect patient confidentiality
- **Principle 8** - Inform patients and service users about how their confidential information is used

**THE GOLDEN RULE**

Just ask yourself - "If this were my personal information, would I do with it what I am about to do?" If the answer is "no" then why would you do it with someone else's? You need to find an alternative approach or identify a lawful basis for processing under UK GDPR/DPA 2018)

## UK GDPR/DATA PROTECTION ACT 2018

There are six data protection principles which regulate the use of personal identifiable data. They are:

1. Processed fairly, lawfully and in a transparent manner.
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and, where necessary, kept to up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary
6. Processed in a manner that ensures appropriate security of the personal data

This means that: -

Personal information given for one purpose must not be used for another without consent or another justifiable legal reason.

Everyone has a right to know what information is being collected and why and to have a copy.

Patients have the right to ask for information not to be shared and when used for reason other than direct care it must be non identifiable.

Staff have a duty to ensure that information is only available to those who have a right to see it.

Staff should understand their responsibility to protect confidential information and to follow the rules and guidance available to them.

The rules are to protect both patients and staff but they should not be applied so rigidly that they are impractical or detrimental to care.

## KEY THINGS TO REMEMBER

All reasonable care should be taken to protect the physical security *of confidential* and *sensitive* (this may also mean "*business sensitive*") information from accidental loss, damage or destruction and from unauthorised or accidental disclosure. This means: -

- Never share or use someone else's login details to gain access to information on computers
- Always lock your computer when it is unattended.
- Data on computers, PCs and laptops should be kept physically secure, held on CCG network drives and be password protected.
- Laptops must have encryption software. No staff or patient information should be stored on CDs, DVDs, USB (memory sticks) or other portable media.
- USB sticks (memory sticks) must be encrypted
- Any confidential or sensitive information must be kept secure and not left unattended where it might be seen by patients/public/staff
- Confidential information should only be faxed when there is no alternative and immediate receipt is essential for clinical reasons. Safe Haven fax is preferable but if that is not available use the procedure described in the Information Governance Policy – you can find this on the CCG staff zone of the intranet site.
- Envelopes containing confidential or sensitive information must be securely sealed, labelled 'confidential' and clearly addressed to a known contact
- Telephone validation procedures must be followed to confirm the identity of telephone callers before confidential information is provided
- The most secure method for transmitting patient identifiable information via email is

both to and from an NHSmail address (xxx@nhs.net) where this is necessary.
- Personal mobile phones should not be used for work e-mails.
- Follow the CCG Information Governance policies and guidance on Confidentiality and Information Security and seek advice when in doubt

## RECORDS MANAGEMENT

All NHS staff are responsible for records which they create or use in the performance of their duties.
Any record that an individual creates is a public record.
Records created by the organisation should be arranged in a record-keeping system that will enable quick and easy retrieval of information.
Each department should have safe systems in place for managing their documents taking into account the legislative and regulatory requirements.
Records should be complete and accurate so that employees or their successors can act appropriately, undertake an audit, and to protect the legal rights of the organisation, its patients, staff and any others affected by its actions.
The CCG Records Management Policy, including retention schedule, is published on the intranet at:
https://buckinghamshireccg.nhs.uk/wp-content/uploads/2015/03/IGPOL004-Records-Management-Policy-BCCG-FINAL-V4.1-20181011.pdf (buckinghamshireccg.nhs.uk)

NHS Records retention periods are available at:
https://digital.nhs.uk/data-and-information/records-management-code-of-practice

CCG Information Governance, Information Security and Confidentiality policies and guidance are available on the CCG staff zone.

See also the Department of Health "Confidentiality: NHS Code of Practice" at: -
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

## FREEDOM OF INFORMATION ACT 2000

The aim of the Act is to encourage openness in the public sector so that decisions about how money is spent, or services provided can be seen and understood.

Any member of the public or staff can ask to see information that is held by the CCG.

The law requires the CCG to respond to a request within 20 working days.

If you receive a request, contact the CSU FOI team immediately.

## CONTACTS FOR ADVICE: -

**Your Information Governance Manager**
**paul.antony@nhs.net**

**Your Data Protection Officer**
**Is Lesley Corfield**
**lesley.corfield@nhs.net**

**Your Senior Information Risk Owner**
**is the Director of Finance**
**Robert Majilton**

**The Caldicott Guardian is**
**Karen West**

**Information Governance Training for all staff is available online at;**
**https://www.consultod.co.uk/login/index.php**

NHS
Buckinghamshire
Clinical Commissioning Group

# Look after it and keep it safe!

# Information Security Advice for Staff JULY 2021