# Confidentiality code of practice

## Purpose of the Code

The use and disclosure of confidential patient information needs to be both lawful and ethical. All employees working in the NHS are bound by a legal and ethical Duty of Confidentiality to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 1998 and, in addition, for health and other professionals through their own professions Code(s) of Conduct.
This means that all employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records, patient referral letters,

Disclosures and sharing of personal identifiable information is governed by the requirements of Acts of Parliament and government guidelines.
This Code has been written to meet the requirements of:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- 1997 Caldicott Report

The principle behind this Code of Practice (Code) is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the practice's policies to secure that the confidentiality code is adhered to.
This Code has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. The Code should be fully read by all staff and may also be used for reference. It is based on the document: *Confidentiality: NHS Code of Practice 2003.*
All staff are responsible for adhering to the code.

## Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including employees, volunteers, agency staff, locums, student placements), their families or friends. It also includes the dental practice's confidential information which might include, for instance, contracts, plans for services and developments or policies and procedures. The range of information which can be withheld as confidential is very constrained by the requirements of the Freedom of Information Act.

This Code will apply however that information is stored. For example - information may be held on paper, CD, Word document, Excel spreadsheet, database or printout, video, photograph or even heard by word of mouth. It includes information stored on portable devices such as laptops, palmtops, mobile phones, digital cameras and data sticks.
Information can take many forms including dental / medical records, audits, employee records, occupational health records etc.

Person identifiable information (PII) is anything that contains the means to identify a person. It includes: -

- Surname
- Forenames
- Initials
- Address
- Postcode
- Date of Birth
- Other Dates (i.e. admission, tests, death, diagnosis)
- Sex
- NHS Number
- N.I. Number
- Local Identifier (i.e. hospital or GP Practice Number)
- Ethnic Group
- Occupation

In certain circumstances items taken from this list, combined with other information, may be sufficient to identify a person e.g.

- Age linked to a diagnosis
- Postcode and the medicine prescribed
- Address and the item of service provided

These examples are by no means exhaustive and other combinations of items may serve the same purpose. All personal information is confidential and deserves the same respect for privacy. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.
Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in Legislation (e.g. sexually transmitted infections, HIV and termination of pregnancy).
Under the Data Protection Act sensitive data includes:

- Race/ethnicity
- Political beliefs
- Religious beliefs
- Trade union memberships
- Physical/mental condition
- Sexuality
- Criminality

Opt-in consent is required to hold this information i.e. that the patient is made aware that we are recording and holding this information and that they agree to this.
During your work you should consider all information to be sensitive, even something as simple as a patient's name and address. The same standards should be applied to all information you come into contact with.

**Using and Disclosing Confidential patient information**

There are a range of statutory provisions that limit or prohibit the use and disclosure of information in specific circumstances, and also a range of statutory provisions that require information to be used or disclosed. Key amongst these is the Data Protection Act 1998 and further details on this are given in the sections below. However there is also a Common Law of Confidentiality which is built up from case law. The key principle is that information confided should not be used or disclosed further than that agreed with the individual giving it.

Finally there are ethical standards often set by the Government or the Professional Bodies. An example is that confidentiality obligations also apply to the deceased and this has now been proven in law as being exempt from the provisions of the Freedom of Information Act under Section 41 – Information Provided in Confidence.

**Using and Disclosing Confidential Patient Information – Patient Consent**

Using and disclosing patient information should be done with the consent of the patient. For the patient to consent they should be provided with:

- A basic explanation of what, why and when information is recorded and what further uses may be made of it.
- A description of the benefits from the proposed use or disclosure.
- A description of how the information will be protected, how long it is likely to be retained and under what circumstances it will be destroyed.
- An explanation of any risks, implications or other outcomes if consent to use or disclose the information is withheld.
- An explanation that consent can be withdrawn or given again in the future.
- Answers to any questions they may have about the use and disclosure of their data.

This should be done when the patient first presents for treatment. Indeed the patient's details (name, address, GP, next of kin, carer information etc) should be checked on these occasions as well.
Consent can be explicit (either orally or in writing) or implied (from the patient's behaviour i.e. accepting treatment. The gold standard is to have consent in writing and signed.

If the patient objects to a use/disclosure of their information (withholds consent) then this should be noted in their case notes. For example, if the patient provides information which should not be provided to their carer/ parent or guardian, this fact should be noted in the record. If the carer/ parent or guardian, with the consent of the patient, later makes a Subject Access Request for the records the information would not be divulged.

In the event that staff cannot answer detailed questions from patients then these should be referred to practice manager who can refer to the Caldicott guidelines.

**Subject Access Requests**

Under the Data Protection Act patients have the right to access to information held about them, including their health records. Indeed, people have the right to information held about them by any organisation. The request must be in writing to the practice manager of the dental practice. Access to information should be provided within 28 days of formal request, and can be made earlier should there be a significant reason for the patient's request, at the discretion of the dental practice. The patient should be informed at the point of a request that a fee may apply. As well as the patient, someone with their written consent, a personal representative, a parent or guardian, by Court Order or someone with a claim arising for the death of the patient may also apply for access to the records.

# Requests for Information on Patients

Never give out information on patients or staff to persons who do not “need to know” in order to provide health care and treatment.

All requests for patient identifiable information from someone who is not the patient and is not involved in his / her care should be on a justified basis and some may also require to be agreed by the practice manager. Any exceptions to this rule may require written consent from the patient in advance.

If you have any concerns about disclosing / sharing patient information you must discuss these with the practice manager and if they are not available, then discuss with the principal dentist. If you cannot find anyone to discuss the issue with, you should take down the caller’s details and ring them back once you have had a chance to discuss the request with an appropriate person and they are satisfied that the disclosure of information can take place.

# Telephone Enquiries

If a request for information is made by telephone, in general:

1. Always try to check the identity of the caller and
2. Check whether they are entitled to the information they request.
3. Take a number, verify it independently and call back if necessary.

Remember - even the fact that a patient is attending the dental practice is confidential.

**Checking Details – the Patient**

Most people wouldn't give a second thought that family and friends would be able to phone the practice to check their location and how they are doing. However there are occasions when people might not want this information divulged e.g. celebrities, witness protection, child protection, family disputes etc.
Similarly many patients have family or carers phone on their behalf to arrange appointments or confirm details. On the other hand there are patients who do not want their nearest and dearest to know about their medical conditions.
The over-riding principle is that it is the patient's information and the practice must act in accordance with their wishes.

When a patient is registered with the practice, details of next of kin, spouse or carer, should be recorded and the patient asked if details may be disclosed to the nominated person in their best interest in the case of an emergency. They should also be asked if there is anyone to whom information should not be divulged or if there are restrictions on the level of information they want to be given out i.e. Fraser competent child does not want details disclosed to parent / guardian. This must be documented in their health records and staff must be made aware in case they take calls enquiring after the patient.

## Appointment queries

Many patients request that other people check the details of their appointment, or change an appointment for them. While this is usually a genuine request, the practice has to safeguard the patient's confidentiality, as they may not wish anyone to know they are attending practice at all, and some relatives / employers may try and discover this information.

1. Ask identity of caller and their relationship to the patient, and verify as far as possible against the patient's data on the records held.
2. Ask the caller to provide the verifying patient details – such as full names, Date of Birth, Address, Post Code, NHS Number, Date of Appointment.
3. If you are in any doubt about the caller's authenticity or reason for the call then do not release information. Take the caller's phone number, consult with the practice manager or principal dentist, before calling back. In certain circumstances it may be advisable to contact the patient.
4. If the above criteria are met the appointment details may be confirmed or re-booked.

# Requests for Information by the Police

Requests for information from the Police, whether in person or by telephone, should always be referred to the Practice Manager or Principal Dentist.

**Guidelines for the disclosure of information relating to patients to police officers in matters involving serious crimes and or serious motor vehicle offences.**

**Purpose**

During the course of an investigation into a possible crime the police may require details and or information about a patient. The practice must ensure that information given is correct, is disclosed appropriately and maintains patient confidentiality.
It is recognised that the practice staff are governed by a duty of confidentiality with regard to information concerning patients and must not voluntarily disclose information without the express consent of the patient. However, there are instances when a request from the Police may override the duty of confidentiality.

**Procedure**

**All requests, whether in person or by telephone, must be referred to the Practice Manager or Principal Dentist. Staff must at all times adhere to the following procedure.**

- Obtain the name, number and status of the enquiring police officer.
- Establish the nature of the enquiry and necessity for obtaining information deemed to be confidential.
- Confirm that the crime being investigated as a serious arrestable offence.
- Record the above information in the general health records.
- Check the identification of the enquirer. If contact is by telephone, then obtain details of the telephone number and police station. Always carry out the ring back procedure to any enquiring Police Officer. Do not reply on any direct line into a Police Station. Only use the official recognised telephone numbers through the switchboard and ask to speak to the enquiring officer.
- Record details of any confidential information released to the police in the relevant health care records. The record must also indicate whether confidential information has been given with or without the patients/relatives consent.
- Should the police wish to interview staff, this should be arranged at a mutually convenient time. Staff should be accompanied by the Practice Manager.

**Note.**
Under the Prevention of Terrorist (Temporary Provisions) Act 1989 S18 it is an offence NOT to voluntarily give information to the Police that may be of material assistance in preventing terrorism or apprehending terrorists. It is therefore unlikely that the duty of confidence in such instances would be sufficient defence for not going to the Police.

## Abuse of Privilege

It is strictly forbidden for employees to look at medical information relating to themselves, their own family, friends or acquaintances unless they are directly involved in the patient's clinical care or administration on behalf of the practice. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

## Carelessness

- Do not talk about patients in public places or where you can be overheard.

- Do not leave any medical records or confidential information lying around unattended. This includes ward or clinic reception desks.
- Make sure that any computer screens, or other displays of information, cannot be seen by the general public.
- Always log out of a computer when you leave it if it is also used by others. If you have sole use, ensure you that you set a screensaver password with a short duration or lock the computer before you leave it.

## Use of External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient i.e. the patient.

## Emailing Confidential Information

The e-mail transmission of this information can pose serious risks to confidentiality (for instance if you send it to the wrong person, or worse still, wrong *group* of people), and should be avoided unless essential to the delivery of health care. In this case strict principles should always be followed.

**Patient identifiers should be removed** where-ever possible, and only the minimum necessary information sent, for instance just the NHS number but no name or address. This in itself can pose problems as the wrong number may be typed. Special care should be taken to ensure the information is sent only to recipients who have a "need to know "; always double check you are sending the mail to the correct person/s.

## Faxing

- Remove patient identifiable data from any faxes unless you are faxing to a known
- Safe Haven (a secure, usually locked and private area which is accessed only by authorised personnel e.g. in a hospital).
- Faxes should always be addressed to named recipient(s).

- Include a fax header sheet which contains the following notice:
- “The information in this fax document is confidential and may be legally privileged. It is intended solely for the addressee. Access to this document by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it is prohibited and may be unlawful. If this document is received by anyone other than the addressee, please contact the sender.”
- Always check the number to avoid misdialling and ring the recipient to check that they have received the fax.
- If your fax machine stores numbers in memory, always check that the number held is correct and current before sending sensitive information.

## Storage of Confidential Information

Paper-based confidential information should always be kept locked away when not in use and preferably in a room that is locked when unattended, particularly at nights and weekends or when the building/office will be un-occupied for a long period of time.

Computer-based information and records should be password protected. Passwords should be rememberable and not recorded in writing and not shared with anyone not employed by the dental practice or an employee where access to such information is not appropriate.

## Disposal of Confidential Information

When disposing of paper-based person-identifiable information or confidential information always use the ‘Confidential Waste’ bins or shredders. Keep the waste in a secure place until you can take it to the Confidential Waste bin or shred it which should be done daily.

## Working at Home

Although not ideal, it is sometimes necessary for employees to work at home. If you need to do this you would first need to gain written approval from the Practice Manager. If they agree, you would need to ensure the following are considered and remember that there is personal liability under the Data Protection Act 1998 and your contract of employment for breach of these requirements:

- Ensure you have authority to take the records as agreed with the Practice Manager.
- If you are taking paper records please ensure there is a record that you have these records, where you are taking them and when they will be returned.
- Please provide an emergency contact number in case the records need to be returned urgently.
- Ensure any personal information in manual form e.g. patient/staff files, or electronic format e.g. data stick/CDs, are in a locked briefcase/pilot case prior to them being taken out of the building.

- Make sure the briefcase/pilot case is put in the boot of the car or carried on your person while being transported from your work place to your home. This must not be left unattended.
- While at home you have personal responsibility to ensure the records are kept secure and confidential. This means that other members of your family and/or your friends/colleagues must not be able to see the content or outside folder of the records.
- You must not let anyone have any access to the records.
- If you take home computer records on a data stick or CD you must ensure all of the above apply. In addition you must ensure if you are putting this information onto your own PC that you take the information off again when you have finished your work.
- Other family members / friends / colleagues must not be able to access this information.
- When taking your records back to work this must be carried out as above, in locked briefcase/pilot case. For manual records they should be logged as being back within the Trust. For computer records on data stick / CD these MUST be virus checked before being loaded onto any of the dental practice's systems.