CONFIDENTIALITY CODE OF CONDUCT

Each member of staff has an obligation to keep information confidential. This code of conduct has been developed to ensure that staff are aware of their obligations and what may happen if these obligations are not met. It is important that staff are aware when they can and cannot disclose information.

YOUR LEGAL OBLIGATIONS

There are legal guidelines as to when information can be disclosed. The legal guidelines have been formulated after extensive discussions and subsequent Acts of Parliament.

The main guidelines are as a result of discussions of the Committee that carried out the Review of Patient-Identifiable Information chaired by Dame Fiona Caldicott and produced the Caldicott Report (published December 1997).

The committee established principles to which we must all adhere to when considering when to disclose information. When considering whether to disclose information we must:

1. **Justify the purpose(s)**
   Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use patient identifiable information unless it is absolutely necessary**
   Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary patient-identifiable information**
   Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to patient identifiable information should be on a strict need-to-know basis**
   Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
5. **Everyone with access to patient identifiable information should be aware of their responsibilities**
   Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. **Understand and comply with the law**
   Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

These principles have been subsumed into the NHS confidentiality code of practice.

The General Dental Council is also clear in our obligations to keep information safe and further guidance can be found in their "Standards for Dental Professionals" at

http://www.gdc-uk.org/Dentalprofessionals/Standards/Pages/default.aspx

OUR CURRENT SYSTEMS AND PROCESSES FOR PROTECTING PATIENT INFORMATION

We have existing Data Protection and Confidentiality Policies and procedures which we are all trained in.

We expect everyone in the practice to observe:

- Records must be kept secure and, in a location, where it is not possible for other patients or individuals to read them.
- Identifiable information about patients must not be discussed with anyone outside of the practice including relatives or friends.
- A school should not be given information about whether a child has attended for an appointment on a particular day. It should be suggested to the school that the child is asked to obtain the dentists signature on his or her own appointment card to signify attendance.
- Demonstrations of the practice's administrative/computer systems should not involve actual patient information.
- When talking to a patient on the telephone or in person in a public area like the reception, care should be taken that sensitive information is not overheard by other patients.
- Do not provide information about a patient's appointment record to a patients employer.
- **Messages about a patient's care should not be left with third parties or left on answering machines.** A message to call the practice is all that can be left.
- Recall cards and other personal information must be sent in an envelope.
- If a patient consents to email and/or text reminders and appointment information and the email address/mobile phone is shared, they must be made aware that other family members with the same email address /mobile phone may see details of that appointment.
- Disclosure of appointment books, record cards or other information should be not made available to police officers or inland revenue officials unless upon the instructions of the dentist.
- Patients should not be able to see information contained in appointment books, day sheets or computer systems.
- No patient information should be disclosed to representatives of NHS England for other such third parties without the permission of the Information Governance Lead, David Baker.
- Discussions about patients should not take place in the practices public areas or within ear shot of such areas.
- There may be occasions when in the routine running of our business, that access to our IT system by third parties is required. Details of these will be provided in the future once computer systems have been installed.

- Access will only be permitted if it is required for hardware or software support. In all instances they cannot access our system without our authorisation. They will guide us through an online procedure which requires us to click that we consent to them accessing our system. You should seek permission from David Baker if you are unsure as to whether to allow access or not.
- If you are allowing access to our hardware provider, please ensure that the workstation being accessed is not logged onto the computer software so as to ensure that they cannot remotely access patient information.
- If you are at all unsure, DO NOT allow remote access.

WHEN CAN INFORMATION BE DISCLOSED?

Responsibility for a disclosure rests with a patients' dentist and under no circumstances can any other member of staff make a decision to disclose.

When it is the public interest

There are certain circumstances where the wider public interest outweighs the rights of the patient to confidentiality. This might include cases where disclosure would prevent a serious future risk to the public or assist in the prevention or prosecution of a serious crime.

Disclosure of Information necessary in order to provide care and for the functioning of the NHS.

In practical terms, this type of disclosure means

- Transmission of claims/information to payment authorities such as the DPD/SDPD/CSA/BSA
- In more limited circumstances, disclosure of information to the NHS England
- Referral of the patient to another dentist or health care provider such as a hospital

Other circumstances

- Where expressly the patient has given the consent to a disclosure
- Where disclosure is necessary for the purpose of enabling someone else to provide healthcare to the patient and the patient has consented to this sharing of information
- Where the disclosure is required by statute or is ordered by a court of law
- Where disclosure is necessary for a dentist to make a bona fide legal claim against a patient, when disclosure to a solicitor, court, or debt collecting agency may be necessary.

WHO TO APPROACH IF YOU NEED A FOR ASSISTANCE AND ADVICE ON DISCLOSURE ISSUES

David Baker is the Information Governance Lead and he will be able to help with any of your questions regarding disclosures.

POSSIBLE SANCTIONS FOR BREACH OF CONFIDENTIALITY OR DATA LOSS

We take a breach of confidentiality or data protection extremely seriously. The Information Commissioners Office can fine us up to £500,000 for a serious breach of data protection. We cannot stress enough how seriously such a breach will be treated.

Staff contracts clearly indicate how serious a breach of confidentiality or data protection is and such breaches may include:

- deliberately looking at records without authority
- discussion of personal details in inappropriate venues
- transferring personal information electronically without encrypting it
- using patient records to obtain information for something other than what is needed

If there has been a breach it could result in immediate dismissal, termination of contract or bringing criminal charges.

For more information you should refer to

- Confidentiality Policy
- Data Protection Policy
- Staff Contracts
- Storage and Disposal of Record Cards Policy
- David Baker

A copy of this policy and all related policies can be found in the policies file on reception which is readily available to all staff at all times.

QUERIES

Queries about confidentiality should be addressed to David Baker.

THIS POLICY IS DUE TO BE REVIEWED ANNUALLY