Information handling procedures

High Street Smiles

1. Introduction

Information is the lifeblood of healthcare services, its proper use and protection is vital to the provision of appropriate care, to maintain the trust of patients in a confidential service and to the success of the practice. It is important therefore that measures are put in place to protect confidential information from unauthorised access or disclosure, loss, destruction or damage.

No matter how it is collected, recorded and used (e.g. on a computer or on paper) confidential information must be used and transferred in accordance with legal requirements, such as the Data Protection Act 2018/GDPR and the common law duty of confidence, and the General Dental Council codes of conduct.

2. Purpose

The Information Handling Procedures are in use to ensure that personal information is protected and that it is not disclosed inappropriately, either by accident or design, whilst in use in the practice, or when it is being transferred or communicated to and from the practice.

3. Scope

The practice collects personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information includes name, address, email address, data of birth, and private, confidential and sensitive information. The procedure applies to all staff including permanent, temporary, and locum members of staff.

4. Secure use of personal information

Guidelines for practice staff on the secure use of personal information are set out on page 4 of this document.

5. Secure receipt and transfer of personal information

We ensures that there are secure points (safe havens), for the receipt of personal information transferred to the practice and has applied the following measures to safeguard personal information during receipt and transfer/transit.

Verbal communications

The practice staff members have been provided with guidance on verbal communications including:

- Taking appropriate precautions not to reveal confidential information e.g. to avoid being overheard when making a phone call; Try not to use names over the phone that may be able to identify(uncommon names)
- Not having confidential conversations in public places or open offices;
- Taking care when leaving messages on patient's answering machines.
- Ensuring contact numbers are correct to prevent information being inappropriately shared and incorrect text messages going to the wrong person

The practice recognises that recorded telephone messages may contain personal or confidential information, for example, names, addresses and health status of patients phoning about appointments; information about applicants for jobs advertised, etc. It has therefore put the following measures in place to protect the confidentiality of this information:

- Only authorised staff members have access to the answering machine;

Postal services and couriers:

To ensure that confidential information transferred from the practice by post or courier is done so as securely as is practicable, the practice ensures:

- Normal post is used for single appointment letters and single referral letters, but for bulk transfers of information, e.g. PR forms, NHS Dental Services, Confidential records, the practice uses tracked and traced post;
- Packaging is "tamper-evident" (i.e. it is immediately obvious if some-one has attempted access the contents) and protects the contents from any physical damage likely to arise during transit;
- Where necessary, additional controls are applied to protect sensitive information from unauthorised disclosure or modification, e.g. the use of locked containers.

Portable devices

The practice is aware of the increased risk to information held on portable devices such as memory sticks, CDs, DVDs, Laptops etc. The practice has therefore put in place the following additional measures for transfer of confidential information held on a portable device:

- Confidential information is not generally stored on hard-drives of laptops and PDAs, and will only be done so if essential for patient care, and even then only for short periods and where the equipment has been encrypted to the appropriate NHS standard;
- Information held on portable devices is only transferred by courier or post if encrypted to NHS standards;
- Devices are properly packaged and clearly labelled to ensure they are handled correctly;
- The password is transferred separately to the device e.g. if the device is posted, the password is sent in a separate envelope or communicated via phone.

Faxes

The practice's fax machine is in a secure location and when receiving faxes containing confidential information, the practice ensures:
Only to be sent if absolutely necessary and not able to use Email

- The fax is removed from the machine on receipt;
- Where necessary, the sender is contacted first on a cover sheet to confirm receipt;
- The information in the fax is appropriately dealt with and safely stored, e.g. transferred to the patient record.

To ensure that confidential information transferred from the practice by fax is done so as securely as is practicable, the practice ensures:

- The fax number is always double checked, and frequently used numbers are stored in the fax machine to reduce the risk of typing errors;
- A fax cover sheet is used and marked "Private and Confidential".
- Faxes are only sent to a named person rather than a team;
- The recipient is informed that a fax will be sent, and asked to confirm receipt;
- Faxes are not sent outside an organisation's working hours where there is no-one present to receive.

Email
Emails received containing patient information are incorporated into the dental record and deleted from the email system when no longer required.

The practice is aware that NHSmail is currently the only NHS approved method for sending patient identifiable information by email, but only if both sender and recipient use an NHSmail account, therefore the practice ensures:

- Email is only used for the transfer of confidential patient information if both parties have an NHSmail account;
- Where NHSmail is used to send sensitive information, this is clearly indicated by the word ‘confidential’ in the subject header.

Other forms of information exchange (e.g. text messages, e-mail, IP phones etc)

6. Approval

These procedures have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	

GUIDELINES ON THE SECURE USE OF PERSONAL INFORMATION

These guidelines apply to all staff including permanent, temporary, and locum members of staff.

If you are working in an area where patient records may be seen you must:

- Shut / lock doors and cabinets as required;
- Query the status of unaccompanied strangers; ID checks if visitors
- Know who to tell if anything suspicious or worrying is noted;
- Not tell unauthorised personnel how the security system operates;
- Not breach security.

If you are using paper patient records you must ensure they are:

- Tracked if transferred out of the practice, with a note made in the tracking register;
- Returned to the filing location as soon as possible after completion of treatment;
- Stored securely within the practice, arranged so that the record can be found easily if needed urgently; (Filed in alphabetical order in a locked cupboard)
- Stored closed when not in use so that contents are not seen accidentally;
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons;

If you are using electronic records, you must:

- Always log-out of any computer system or application when work on it is finished;
- Not leave a terminal unattended and logged-in;
- Not share logins with other people. If a colleague has a need to access patient records, then appropriate access should be organised for them – this must not be by using your access identity;
- Not reveal your password to others;
- Change your password at regular intervals;

- Avoid using short passwords, or using names or words that are known to be associated with you, e.g. your favourite football team, your name;
- Always clear the screen of a previous patient record before seeing the next patient;
- Use a screensaver (preferably with password) to prevent casual viewing of confidential information by others.

When communicating information about a patient you must **take care**:

- Not to discuss patient information in public areas;
- If transferring information by phone, or face to face that personal details are not overheard by other people, including staff who do not have a “need to know”;
- When leaving a confidential message on a patient’s answer-phones as it might be heard by someone other than the intended recipient;
- If listening to answer-phones messages that they cannot be overheard by unauthorised persons;
- When receiving calls requesting personal information and make sure to verify the identity of the caller (see below), ask them why they want the information and if in doubt about whether the information can be disclosed, tell the caller you will call them back, and then consult with your manager;
- Not to leave messages containing personal information on notice boards that could be accessed by non-authorised staff.

To verify the identity of a caller requesting personal information:

- Ask them for their phone number;
- Check that it is the correct number for that individual or organisation;
- If it is, call them back once you have decision on whether the information can be disclosed.
- Ask for signed written consent for requests (See Confidentiality policy, Data protection privacy notice)

Transferring patient information

If you are authorised to transfer patient information you must only do so in accordance with the procedures set out in the **Information handling procedures (see pages 1 - 3 of this document or if the procedure has been separated from these guidelines)**

Approval

These guidelines have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	