Clinical examination & record-keeping: Part 3: Electronic records

A. M. Hadden[1] and the FGDP(UK) Clinical Examination and Record-Keeping Working Group

In brief

Discusses the creation and maintenance of electronic records.

Advises on security and encryption for electronic records.

Discusses the legal aspects of retaining electronic records in practice.

This article is the third and final part of a *BDJ* series of Practice papers on the subject of clinical examination and related record keeping. The series is taken from the Faculty of General Dental Practice UK (FGDP[UK]) 2016 Good Practice Guidelines book on this topic, edited by A. M. Hadden. This particular article covers the creation and maintenance of electronic patient records, including security and encryption guidance. It is important to note that throughout this article (and the *BDJ* series and associated FGDP[UK] book), the specific guidelines will be marked as follows: **A:** Aspirational, **B:** Basic, **C:** Conditional. Further information about this guideline notation system is provided in Part 1 of this series (*BDJ* 2017; **223:** 765–768).

Introduction

Electronic records are now widely used in medical and dental practices, and there is the increasing possibility to move towards a 'paperless' practice. While generally they can do the same as paper records, there is the capability of pulling together an integrated patient record and practice management system with a wide range of facilities, all in one place. This can include patients' clinical records, diagnostic imaging, patient reminders, treatment plans, along with management systems, such as appointments, accounts, correspondence, and laboratory prescriptions.

[1]Dento-legal adviser and General Dental Practitioner
Correspondence to: Dr Andy Hadden

Accepted 15 September 2017
DOI: 10.1038/sj.bdj.2017.994

Clincial Examination & Record-Keeping*

Part 1. Dental Records
Part 2. History Taking
Part 3. Electronic Records

*This series represents chapters 2, 3, and 8 from the FGDP(UK) Good Practice Guidelines entitled *Clinical Examination & Record-Keeping*, which is available online at https://www.fgdp.org.uk/guidance-standards. The content herein is reproduced with kind permission of FGDP(UK).

Many software programs available allow remote access to files, as well as structured templates to suit the individual clinician. Electronic records offer many advantages, including legible notes, but also come with some disadvantages.

The principles of the entries in electronic records are identical to those referred to earlier in this book.

From the list in Part 1 of this *BDJ* series (chapter 2 in the FGDP[UK] Guidelines), the following variations apply to electronic records:

- Ensure all entries are dated, timed and the clinician and assistant are identified.
- Any errors should be identified by a later correcting entry, which refers to the error.
- When a printout is required, ensure pages are numbered and identifiable by name and identifier such as the address or date of birth of the patient.

When printing out electronic records, all data that can be reasonably printed out should be done. Printing of selective data can cause problems in assessing the care undertaken. An example is the printing out of 'void entries' where amendments had to be made to records. The software must allow the printing in full of all items of the dental record as detailed in Part 1 of this *BDJ* series (chapter 2 in the FGDP[UK] Guidelines).

The clinician should be familiar with the system used, and be able to locate and understand the information that has been entered.

Security

Any electronic system must be secure, regularly backed-up, and allow access only to those who require the information to perform their duties. Each user must have a unique password. For maximum security, passwords should contain mixed-case letters and include numbers or symbols and should be changed regularly. Passwords should not be written down and kept under keyboards or on desks or surfaces where the public may be able to access them. There may be differing level of access, such as clinician, receptionist, manager, owner, etc. Administrative functions can be reserved only for a specific person, thereby helping reduce the risk of accidental alterations of the system settings that may result in data corruption. For data stored on a central server, similar security measures should be employed. Firewall and antivirus software should be employed for

Faculty of General Dental Practice - Good Practice Guidelines

The Faculty of General Dental Practice (FGDP[UK]) provides evidence-based guidance and standards for the whole of the dental profession in order to promote high quality practice and patient care. Their publications are available in variety of formats including hard copy, e-books, and free of charge online as part of the Open Standards Intiative.

Clinical Examination and Record-Keeping is a complete reference guide to record-keeping and examination, and is available in hard copy and free of charge online. The hard copy includes scenarios to put the guidance into context, as well as a series of extensive appendices, diagrams, charting notes and template forms which dental and professionals may adopt for use in their practice.

The FGDP(UK) published its newest guidelines, Dementia-Friendly Dentistry: Good Practice Guidelines in October 2017.

For more information about all FGDP(UK) standards and guidance, visit: www.fgdp.org.uk/guidance-standards

computers or servers (including external servers) connected to the internet, and consideration should be given to encrypting data that is transmitted between the practice and the server. Practices are advised to seek external specialist advice as required.

A full audit trail facility must be present to prevent the overwriting, erasure or corruption of data. The system should be backed up daily, and a copy retained at separate premises, and protected from fire, flood, and theft.

In an area where anyone other than the patient could see the screen, the computer should be sited so the screen is not easily seen by patients. There should be screen closure after a short period of inactivity to ensure that someone inappropriate does not look at the screen if the monitor is unattended after activation.

It is not within the scope of this book to describe electronic record systems and software fully, and clinicians should ensure that any system they use allows them to meet their legal obligations and statutory requirements.

Other aspects of the system requirements will be referred to under the relevant topics below.

Identifying who made an entry

It should be possible to identify who has made entries in the records, including the date and time. A clinician should ensure that any entries are confirmed as correct and 'signed off' prior to being locked into the system as it is difficult to modify entries subsequently should any error have occurred.

Contents of electronic records

As noted earlier, electronic records can retain a lot of data about patients: clinical, as well as what can be described as 'management'. The list of clinical items is described in Part 1 of this *BDJ* series (or chapter 2 in the FGDP[UK] Guidelines). To this can be added items that would not always be included in a handwritten record, such as a patient's appointments, history of cancellation, payments for treatment, capitation scheme payments, etc. This guidance will refer to the components related to clinical examination and record-keeping.

History taking

Pre-examination

The information detailed in Part 2 of this *BDJ* series (or chapter 3 in the FGDP[UK] Guidelines) should be gathered. This may be inputted directly onto the computer by a suitably trained assistant. If a form is completed and signed by the patient, it can be scanned into the computer.

Medical history

This should be obtained as outlined in Part 2 of this *BDJ* series (or chapter 3 in the FGDP[UK] Guidelines). The principle of this information being verified by the patient remains, and the clinician should be able to demonstrate that they have reviewed the details provided by the patient. This can be done in several ways, and include the following methods:

- The patient and clinician can provide electronic signatures (not every system will have this available). Steps should be taken to ensure that these cannot be altered, and provide an accurate representation of a patient's signature which can be checked by the patient at the time of signing.
- The patient can complete a form as in 3.3, which will include the date, signature of patient and dentist, and this can be scanned into the system. At subsequent courses of treatment, this form can be printed, given to the patient, and changes to medical history noted, if any. The form can then be dated and signed as before and scanned into the system.
- An entry can be written in the notes to confirm the clinician has noted the details and, where necessary, clarified with the patient.
- The electronic system should allow the clinician to demonstrate that the medical history has been recorded, verified and clarified with the patient. The system should hold an audit trail confirming entries have been made on the relevant page at the appropriate date.

Socio-behavioural history

The entries in the electronic system are as outlined in Part 2 of this *BDJ* series (or chapter 3 in the FGDP[UK] Guidelines).

Previous dental history

The entries in the electronic system are as outlined in in Part 2 of this *BDJ* series (or chapter 3 in the FGDP[UK] Guidelines).

Full examination

The patient examination is carried out in the manner described in chapters 3 and 4 in the FGDP(UK) Guidelines. The details should be entered in the system and the clinician should be able to locate the information readily. Some systems provide a template for recording findings, and it is for the clinician to decide if such detail is required. In some cases an 'autofill' may be used and the clinician should ensure that the information is relevant and accurate. The contents of an 'autofill' may include details about soft tissue examination, oral hygiene and tooth brushing. Some aspects are detailed below as their style of entry may differ from a handwritten note.

Extra-oral examination

The sites referred to in chapter 4 in the FGDP(UK) Guidelines should be examined and the findings, if any, noted. It should be recorded if no abnormality was found. A clinician may wish to use a template to record findings, including negative findings.

Intra-oral examination

A clinician may wish to use a template to record findings, including negative findings, in detail, such as different sites of the oral mucosa. Some systems allow for a diagram of any lesion to be inserted. Consideration should be given to including a photograph of any lesion with appropriate consent. The examination must be recorded as being carried out, and the presence or absence of abnormality noted.

Hard tissue – tooth examination

The information as detailed in chapter 4 in the FGDP(UK) Guidelines should be recorded. There are various types of charts on which to record this information. They will allow recording of items including charting of teeth, current restorations, caries, and mobility. Some programmes allow recording of toothwear, however, one of the problems of electronic charting is that a diagrammatic or stylised representation is shown in a standard shape and form rather than allowing the facility to create a precise representation of the actual situation. This may require an explanation in the text if the situation is not clear, such as clarification of how much of a tooth surface may be decayed or missing. This is important for future monitoring of lesions. The nature of any prostheses may require to be inserted in the text.

It may not be possible to include endodontically treated teeth in the chart and it is recognised that it is not necessary to expose a radiograph only for this information.

Periodontal considerations

The recording of a BPE is important and can be difficult to locate on some programmes. It is equally difficult to reproduce when records are printed. The clinician should note how to ensure this data can be recorded and reproduced.

Radiographs

There are many systems for digital radiography and the reader is referred to FGDP(UK)'s publication, Selection Criteria for Dental Radiography.[1] As radiographs can be electronically modified, it is important that the system should note the original radiograph, including date and time, along with a marker icon for any enhanced or modified radiograph.

Treatment plan

After the treatment plan has been established, it should be noted in the system. Prior to this, there should have been discussion of options, risks and benefits, including the option of no treatment. This is part of the process of obtaining valid consent as described previously. The treatment plan should be given to the patient and a signed copy retained.

It is important that this plan can be reproduced. In some systems this is not easy to establish. The reason for this is that the plan is on a chart, which is automatically modified once treatment has been entered as complete. Clinicians should ensure that they are able to reproduce an original treatment plan of any previous course of treatment.

Recall examination

This is carried out as described in chapter 5 in the FGDP(UK) book. Any update of pre-examination information should be recorded, and if an assistant enters these details, the clinician should confirm he is aware of any amendments.

Medical history

This should be checked and any change noted. In some systems this is done verbally, and it is important that the audit trail can confirm the check has been carried out. The system should NOT delete the previous medical history as this may require to be reproduced later if investigation of any complaint arises.

Extra-oral and intra-oral examinations

The extra-oral and intra-oral examinations should be carried out as described in chapter 5 of the FGDP(UK) book and the information recorded as outlined previously in this article.

Emergency appointments

The principles in chapter 6 of the FGDP(UK) book should be followed, noting the considerations referred to therein. It is important to record the detail of any soft tissue lesion, as described in chapter 4 of the FGDP(UK) Guidelines.

Referral to other clinicians

Electronic records make it easier to have templates prepared and utilised for various clinical situations, particularly referrals. The principles in chapter 7 of the FGDP(UK) book should be followed. The letter and subsequent correspondence from other clinicians can be retained on the system and easily located.

Disadvantages

Care should be taken to ensure that there are no contradictory or meaningless entries. This can inadvertently occur when templates or autofills are used. The writer should ensure the accuracy and relevance of any entry. The treatment carried out may, for good reason, have varied from the more commonly carried out treatment to which the template refers, and instead of amending the template, the clinician has recorded the actual treatment carried out, for example a different material for a temporary crown. This makes it difficult to recall detail several years after the event and can devalue the integrity of the records.

If there is a failure of the system, it is difficult to carry out the intended treatment for a patient without notes. Care should be taken, particularly to reassess the medical history and treatment plan, if proceeding in this situation.

Retention of records

The Data Protection Act states that records should be 'not kept longer than is necessary'.[2] The Department of Health guidance suggests this is no longer than 30 years.[3] However, with electronic record systems this may be difficult due to obsolescence of hardware and systems. As with paper records, arrangements should be made to retain records for a minimum of 11 years from when the patient last attended the practice, or age 25 for children (whichever is longer). When disposing of a computer, it is necessary to ensure information has been deleted from the hard drive and advice should be sought about safe and compliant data destruction.[4] It may be necessary to physically destroy the computer's hard drive in order to ensure that no patient data may be recovered using specialist software.

Practices that are closing must inform patients of the date on which the practice will cease trading, and inform patients of how they may request their records or ensure their records are transferred to another practice.

Encryption of records for transfer

When transmitting or transferring patient records electronically, all practical steps should be taken to ensure that only the intended recipient can access the data.

Patient records, whether transmitted by email or saved onto a portable storage device such as a memory stick, should as a minimum be password protected. The password(s) must be communicated to the intended recipient separately and in a secure manner.

End-to-end encryption offers a greater degree of security than password protection.

However, it is only a viable option if both the sender and recipient use the same encryption software. In some circumstances, such as referral to other healthcare bodies/practitioners, this may be possible and its use would be preferable.

Practices are advised to seek expert advice on the most appropriate means of ensuring the security of transmitted data for their particular IT infrastructure configuration.

The practice should have a written policy governing the security of all electronic communications, and the protection of data therein.

1. Faculty of General Dental Practice (UK). Selection Criteria for Dental Radiography, 3rd edition. London: Faculty of General Dental Practice (UK), 2013.
2. Data Protection Act 1998. London: HMSO; 1998. www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf.
3. Department of Health. Records management: NHS Code of Practice Part 2, Annex D1. London: DH, 2009. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf.
4. https://www.microsoft.com/security/online-privacy/safely-dispose-computers-and-devices.aspx.