Dartmouth Dental Practice Procedures

TO: **All Surgery Staff**

FROM: **Marian Roberts**

DATE: **Sunday, 21 July 2019**

SUBJECT: **Access Management of Computer Based System**

Scope of this procedure

This procedure describes how we control access to sensitive patient information. All systems are administered by the practice manager - Keith Roberts. We regularly review the security of our systems for their security and integrity. We use Two Factor Authentication (2FA) wherever possible. 2FA requires a username, password and then an authentication code which is sent to a separate device (mobile smart phone). Only with these 3 elements can access be gained. Wherever possible an audit trail is recorded whenever access is made to our system (Dentally) which reveals the date, time and the user accessing, viewing and changing information.

A number of systems are used by the practice to access patient information. These systems fall into three categories

- **Custom built databases designed and built by the practice**
  - Direct Debit collection from patients (password protected for both database and individual users)
- **Systems supplied by a third party supplier**
  - Planmeca Romexis Clinical Imaging Software
- **Systems provided by suppliers with access being obtained through the internet**
  - Dentally - Practice Management Software.
  - HSBC banking application.
  - Bottomline Technologies PTX - Direct Debit Payment and Collection software.
  - BACS - (Banks Automated Clearance System) - allows us to monitor direct debit collection.

Planmeca Romexis Clinical Imaging Software is held on a central server at the practice. Information held on this system includes:-

- patients ID number

- patients first name
- patients family name
- patients date of birth
- patients gender

The data is integrated with Dentally our practice management software. It is possible to access this information remotely but the same 2FA process has to be followed.

Technical access controls

1. Dentally (Practice Management Software) is at the core of our data systems and user 2FA to gain access.
2. Patient list - access through computer password system built into operating system by Apple Computer Corporation.
3. Direct Debits for Patients - access through computer password system built into operating system by Apple Computer Corporation. Authentication is required whenever the system is accessed.
4. The patient x-ray database (Planmeca Romexis Clinical Imaging Software) is a multi user system. Access through computer password system built into operating system by Apple Computer Corporation.
5. HSBC banking application - access through computer password system built into operating system by Apple Computer Corporation and access to database has additional password access controls - username, password and pseudo randomly selected access codes. A ‘dongle’ is also needed to gain access to banking information. The dongle generates a pseudorandom 6 digit authentication code every time access is needed which has public and private end to end encryption.
6. BACS direct debit collection system - access through computer password system built into operating system by Apple Computer Corporation and access to database has additional password access controls - username, password and pseudo randomly selected access codes. Password changes required every 6 months.

Procedure for granting access

The Practice Manager administers all access to computer systems but does not have access to individuals passwords and 2FA devices.

Procedure for managing changes in access rights

The procedure also needs to cover the process for changing access rights, for example if the user is on long-term leave, or leaves the organisation, their profile would need to be suspended or removed.

Procedures for staff in relation to logging into the system: Systems may provide password protection features such as:

1. users must change their password after the first logon;
2. users must specify complex passwords;
3. users must change their passwords periodically;
4. prevention of password reuse;
5. users may change their password at their request.