ROOT CANAL
DENTAL REFERRAL CENTRE

1 February 2017

# Data protection policy – security of personal data held by the practice

This policy describes Root Canal Dental Referral Centre's procedures for ensuring the security of personal data held by the practice. It should be read in conjunction with our Data Protection Policy and Confidentiality Policy.

## Confidentiality

In order to ensure confidentiality, we take the following measures:

- All staff employment contracts contain a confidentiality clause.
- Access to personal data is on a "need to know" basis only. Access to information is monitored and breaches of security will be dealt with swiftly by the Dr Nicolai Orsteen.
- We ensure that personal data is regularly reviewed, updated and deleted in a confidential manner when no longer required. Where a person ceases to be a patient of the practice, we keep patient records for at least 11 years or until the patient is aged 25 – whichever is the longer.

For further information, please refer to our Confidentiality Policy.

## Physical security measures

In order to ensure that data we hold (whether on paper records or on computer) remains physically secure, we observe the following rules:

- Personal data may only be taken away from the practice premises at Upper Ground Floor, 351 Richmond Road, East Twickenham in exceptional circumstances and with authorisation from Dr Nicolai Orsteen. If personal data is ever taken off practice premises, it must never be left unattended in a car or public place.
- Are stored on computer. The only patient information retained on paper are the medical history forms, which are retained to allow re-signing on subsequent visits, and original incoming correspondence (eg letters), which must be retained for medico-legal reasons notwithstanding that this is also scanned into the computerised records. A lockable cabinet is provided in reception to store these. Archived records are stored securely in the practice office. This makes our paper records inaccessible to patients or other visitors to the practice premises.
- The practice premises are secured when not in use. All doors have at least two locks or bolts. Locks are re-keyed at regular intervals following changes of keyholder staff. The practice windows also have security locks. The practice also has a comprehensive security and fire alarm system, which is linked to a remote monitoring service that automatically summons keyholders, the police or the fire brigade, as appropriate, in the event of an intrusion or fire.

- The practice has a business continuity plan in place which will be implemented in case of a disaster (eg fire, flood, earthquake, tsunami, hurricane), which includes procedures for protecting and restoring personal data.
- When physical patient records are destroyed, this is done in a secure fashion: written records, correspondence, photographs, x-ray films and mounts are shredded using a cross-cut shredder for maximum security.  This may also be sub-contracted to a suitable confidential waste contractor such as xxx.

## Information held on computer

Information held on computer requires particular precautions.  We follow these procedures to protect it:

- The practice uses passwords to protect computerised records.  These are known only to the people who require access to the information.  Staff are instructed never to write down passwords.
- Staff using computers are given training in how to avoid unintentional deletion or corruption of information.
- Computer system users are granted access to system functions only where they are strictly necessary to perform the particular functions of their job.  Administrative functions are reserved to the Practice Owner only, reducing the risk of accidental alterations to system settings that may result in data corruption.
- Specialist dental computer software used for maintaining clinical records has a full audit trail facility to prevent the overwriting or erasure of data.  The software records details of any amendments made to data, who made them and when.
- The practice computer system is protected by antivirus and firewall systems in order to minimise the risk of unauthorised access, data corruption or data loss.  These are updated automatically and checked on a monthly basis to ensure the software and the definitions it uses are the most recent versions (refer to Equipment Testing and Maintenance Schedule).
- The practice computer system operating system software is updated automatically (refer to Equipment Testing and Maintenance Schedule) so as to minimise system vulnerability to viruses, trojans and other malware and to reduce the risk of unauthorised access, data corruption or data loss.
  - We operate several systems of backups and redundancy to ensure that data is not lost: (i) we have mirrored hard-drives so that all data is simultaneously stored *in real time* on two separate hard drive units in case one should fail; (ii) the dental software program is cloud based and is securely stored according to the software provider (see https://dentally.co/security/); (iii) all clinical data stored on the server is copied to the office computer every night using a network backup system; (iv) we operate an automated, encrypted daily "cloud" backup that copies all critical data.