****

**Data security policy**

Lighthouse dental practice is committed to ensuring the security of personal data held by the practice. This policy is issued to all staff with access to personal data at the practice and will be given to new staff during their induction. If any member of the team has concerns about the security of personal data within the practice they should contact Mohamed Elbadri.

All members of the team must comply with this policy.

# **Confidentiality**

* All employment contracts and contracts for services contain a confidentiality clause, which includes a commitment to comply with the practice confidentiality policy
* 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 Mohamed Elbadri.
* We have procedures in place to ensure that personal data is regularly reviewed, updated and, when no longer required, deleted in a confidential manner. For example, we keep patient records for at least 10 years or until the patient is aged 25 – whichever is the longer.

# **Physical security measures**

* Personal data is only removed from the practice premises in exceptional circumstances and when authorised by Mohamed Elbadri.If personal data is taken from the premises it must never be left unattended in a car or in a public place
* Records are not kept overnight without being shredded or securely locked away, as all records should be scanned and left digitally on the patient's file.
* Efforts have been made to secure the practice against theft by, for example, the use of intruder alarms, lockable windows and doors
* The practice has in place a business continuity plan in case of a disaster. This includes procedures for protecting and restoring personal data.

# **Information held on computer**

Appropriate software controls are used to protect computerised records, for example the use of passwords and encryption. Passwords are only known to those who require access to the information, are changed on a regular basis and are not written down or kept near or on the computer for others to see

Daily and weekly back-ups of computerised data are taken and stored in a fireproof container, off-site. Back-ups are also tested at prescribed intervals to ensure that the information being stored is usable should it be needed

Staff using practice computers undertake computer training to avoid unintentional deletion or corruption of information

Dental computer systems have a full audit trail facility preventing the erasure or overwriting of data. The system records details of any amendments made to data, who made them and when

Precautions are taken to avoid loss of data through the introduction of computer viruses.

# **Loss of patient information**

Any loss, damage to or unauthorised disclosure of patient information must be reported immediately to Mohamed Elbadri.

By: T Hale

Date:22.02.2021

Review date:22.02.2022

**NOTE:**

**IF WE CHANGE FROM R4 AND GO TO A CLOUD BASED SYSTEM, WE WOULD NEED TO ADD THIS STATEMENT TO OUR POLICY: Data stored on cloud computing facilities has in place a rigorous service level agreement with our cloud provider to ensure that all our obligations in this policy are fulfilled and that all information is secure.**