Information Security Policy

The Pepper Clinics

1. General

The Pepper Clinics takes seriously its obligations, both in law and against professional standards, to maintain a high standard of security around all data which it holds and processes, and particularly personal and special (health) data (as defined in the Data Protection Act 2018 and the General Data Protection Regulation (EU)).

- Kamlesh Makwana - Contact Details 01733 341777
  is designated as the Information Security Officer for the practice

All issues related to Information Security shall be reported to the information Security Officer without delay.

2. Access to Personal Data – Digital

All employees and contractors with access to personal data held by the practice must adhere to the following requirements:

(a) A personal log-in and secure password (as approved by the practice) must be used on each occasion that digital data is accessed
(b) Under no circumstances shall the password be divulged to any other person nor shall it be written down or stored on any device
(c) Passwords must be changed at the following intervals 6 weeks.
(d) No personal data shall be accessed or processed in any way other than for the purposes it was obtained as set out in the practice's Privacy Statement
(e) All computers and other devices must be locked to a secure screen-saver mode when not in active use
(f) Computers and other devices shall not be used so as to permit any unauthorised viewing or processing of personal data
(g) No personal data shall be copied, downloaded or transmitted to any device or storage medium other than those authorised by the Information Security Officer
(h) No applications, programs or other functionality shall be downloaded or placed on any practice computer or device other than those authorised by the Information Security Officer
(i) Extreme care shall be taken when opening any file attachment originating outside the practice and in any case of doubt the Information Security Officer shall be advised before so doing
(j) No information about practice systems, log-in or other technical details may be provided to any person without the authority of the Information Security Officer
(k) No device or computer may be connected to the practice internet router or any server without the prior consent of the Information Security Officer

3. Environmental Security

All employees and contractors of the practice must adhere to the following requirements to ensure that the practice maintains security around personal data:

(a) All patient records, radiographs, correspondence and other items which can identify an individual person shall be kept in a secure location which is locked or suitably protected from unauthorised access as approved by the Information Security Officer
(b) The practice premises must be securely locked against unauthorised entry when closed and any alarms must be set and checked by those authorised to do so
(c) All desks and work surfaces shall be cleared of material which could identify an individual person when not in use including telephone and other notes
(d) Incoming telephone recording messages shall be cleared and deleted from the system once they have been actioned
(e) No material which can identify an individual person shall be left in such a position that it can be viewed by unauthorised people

4. Internet and External Security

The practice will apply suitable security programs to all systems so as to prevent the introduction of malware or allow unauthorised access, including but not limited to firewalls and anti-virus software as approved by the Information Security Officer and/or the Technical Support Adviser. All software, including the above, will be regularly updated as required.

Penetration testing of the computer, security and telephone systems may take place at intervals and may not be advised in advance to staff and contractors who should therefore maintain vigilance at all times

5. Data Back-up

All personal data will be backed-up on a daily basis using personnel, processes and devices as approved by the Information Security Officer. Back-ups will be audited and confirmed as effective on a regular basis.

6. Off-site Data and Security

Where the information Security Officer has authorised that any personal or other data may be taken or transferred off-site (outside the practice location):
(a) All such authorisations shall be written and a record kept
(b) Authorised data and devices shall be used only for the purposes and period authorised
(c) The requirements in Clause 2 of this Policy will apply to all such instances
(d) Any loss or damage to devices or data must be *immediately* reported to the Information Security Officer and a Data Breach notification template prepared
(e) Devices and data must be secured and out of sight to unauthorised persons whilst in transit and shall be kept in a locked environment when not in use

7. Financial Data

When digital payments are taken from patients or other parties at the practice, all staff or contractors will:
(a) Ensure that the requirements of the EFTPOS (Electronic Funds Transfer – Point of Sale) device/s and systems supplier are followed at all times
(b) Ensure that PCI (Payment Card Industry) best practice guidance is followed
(c) Take all precautions against fraud or misuse of payment cards
(d) In particular ensure that no payment card details are written down

8. Internet and E-mail Use

All staff and contractors will follow the practice rules for use of the internet and e-mails and adhere in particular to any requirements or restrictions on:

(a) Personal internet browsing
(b) Sending or receiving personal e-mails
(c) The encryption of authorised practice e-mails containing patient or other personal data

9. Destruction of Data

Data shall only be destroyed with the explicit written consent of the Information Security Officer and using methodology which is secure and approved. Paper data such as notes, jotters which contain personal information will be shredded on the premises or using an authorised contractor.

Devices to be de-commissioned will have all data securely removed from them using an authorised contractor: it is acknowledged that routine formatting or factory re-setting will not suffice.

10. Other

All staff and contractors shall at all times take utmost care and diligence in protecting all data, including personal and health-related data, within the practice.

The practice undertakes to regularly train and update staff on the processing of data held, whether digital or otherwise in order to assure the competence of all users and maintain awareness of data protection and information security.

All and any concerns about the security of data held by the practice, however apparently slight, shall be brought at once to the attention of the Information Security Officer and it shall be the policy of the practice that any such information shall be positively and constructively received to encourage prompt and vigilant awareness of the importance.

Any breach of the terms of this policy may lead to disciplinary action against staff or contractors and repeated or serious breaches may be regarded as serious misconduct resulting in termination of employment or engagement.

March 2019

Review March 2020