New Dover Road Surgery

IG & Security Policy

Reviewed July 2019

1. Policy Statement

1.1 As the Practice becomes increasingly reliant on computerised systems for communications and for information management, associated risks increase.

1.2 Such risks may range from management of systems and infrastructure, control and application of computer software, and corruption or disclosure of the data processed.

1.3 This policy sets out to identify the broad areas of risk to be addressed and the manner in which those risks should be addressed.

1.4 The implementation of this policy within the practice will take account of local circumstances and risks but will specifically address the points detailed in this document.

1.5 This policy draws upon and conforms to guidance laid down in the NHS IM&T Security Manual (1999)

2. Scope

This policy is concerned primarily with the management of risks associated with computerised systems and the associated infrastructure. These can be broadly stated as follows:-

2.1 Preservation of confidentiality

Promoting a culture that values the confidentiality of personal information and establishing appropriate controls to protect confidentiality.

2.2 Maintaining Integrity of Data

Establish controls to protect data from accidental or deliberate loss or corruption.

2.3 Ensuring Availability of Systems and Data

Providing and maintaining hardware, software and network facilities to provide practice staff with access to the information and services they need

2.4 Maintaining Business Continuity

Establishing appropriate contingency plans to cover major loss of systems or data.

2.5 Avoiding Prosecution

Establishing appropriate controls over software installation to ensure that the practice does not breach the terms of its software licenses

3. Responsibilities

Overall responsibility for security and confidentiality issues within the practice rests with the designated partner or partners. Specific areas of responsibility may be delegated to colleagues or other members of staff if appropriate.

Specific responsibilities include:

Security Manager (Practice Manager)

The Security Manager is the person responsible for reviewing Practice compliance with the Security Policy, and advising the Practice on measures required to achieve compliance. Some other specific responsibilities are mentioned in the body of this policy. The Security Manager will be the point of contact between the Practice and the CCG or Commissioning Support Unit (CSU) on IM&T security matters.

System Manager (Practice Manager)

The System Manager is the person with day-to-day responsibility for the Practice network and the Practice computer system. The system manager will be responsible for establishing access control procedures and will be the point of contact between the Practice and the system supplier, and between the Practice and the CCG or CSU, on operational issues.

Caldicott Guardian (Dr G Robinson)

The Caldicott Guardian is the person with responsibility for ensuring that adequate arrangements are in place to ensure confidentiality of patient information, in accordance with the recommendations of the Caldicott report. The Caldicott Guardian will be the point of contact between the Practice and the CCG or CSU on matters relating to the implementation of Caldicott recommendations.

Data Protection Officer (Practice Manager)

The Data Protection Officer is the person with responsibility for ensuring that the Practice complies with the requirements of the Data Protection Act 1998 and, in particular, for maintaining up to date "notification" to the Information Commissioner. The

Data Protection Officer will be the point of contact between the Practice and the CCG or CSU on matters relating to the Data Protection Act.

More information on the Data Protection Act can be found at **http://www.informationcommissioner.gov.uk/**

Data Owner (All Doctors)

The Data Owner is the person (or persons) responsible for a specific set of patient records. This policy is primarily concerned with the electronic records on the practice computer system and the patient's paper records, so the role of data owner may be synonymous with that of the system manager or records manager. The Data owner will be responsible for ensuring that access restrictions and other controls are enforced.

All Practice staff are expected to read and comply with the Security Policy

4. Information Security

4.1 System and Network Access Controls

Access to the Practice network and systems will be granted only to named individuals.

Each user must be assigned their own unique user ID and password. They may also have been issued with a NHS smart card to access IT services. Log-in and password controls must be suitably configured where systems provide these features. Controls should specify (as a minimum) password length, password expiry, number of acceptable failed logins, number of grace logins. Each user's privileges should be restricted to those required to perform their duties. A user account must be disabled immediately if the user leaves the employ of the Practice. If the individual is moving within the NHS their smart card will need amending by the CSU, but if they are leaving the NHS completely their smart card will be returned, with the appropriate paperwork, to the CSU for disposal.

4.2 Data Authentication and Accountability

Data entry into the practice system will be restricted to properly trained and authorised users. The practice will maintain a register of users who are authorised to make entries on behalf of others. Entries must be ascribed to the healthcare professional who wrote or dictated the notes. Individual members of staff will be held responsible for the content and accuracy of information that appears to have been entered by them or on their behalf. Where systems provide an audit trail facility, this should be enabled. Where reports or correspondence are received electronically or otherwise from outside the practice, appropriate procedures will be implemented to ensure that the information is:

- From an approved source.
- Complete and accurate.
- Promptly merged to the relevant patient record.

4.3 Virus Protection

Anti-virus software will be installed and enabled on all personal computers and notebooks/laptops used for Practice business. This includes computers that may be used outside of practice premises (home computers used for practice business). The anti-virus software will be regularly updated. The Security Officer will report any potential computer virus threats to the CSU.

4.4 Hardware and Media Disposal

The Security Officer will implement appropriate procedures to ensure that personal or sensitive data is not inadvertently disclosed when hardware or media, is relocated, sold or otherwise disposed of. They should contact the CSU for advice on disposal

5. Physical Security

The Security Officer will assess and implement physical security measures appropriate to the nature of the Practice and the level of perceived risk. The areas to be assessed should include the following:

5.1 Access controls

Key equipment (e.g. servers & communications equipment) and paper records should be located in an area to which access can be restricted and monitored during practice hours. If possible, a lockable room or cabinet should be used. The premises should be adequately secured, and preferably alarmed, when the surgery is closed.

5.2 Environmental controls

Key equipment and paper records should be located in areas with appropriate environmental controls to reduce the risks from excessively high or low temperatures, humidity or dust. Fire risk should be minimised by the use of smoke detectors and alarms.

Areas where there is a risk of water spillage or flooding should be avoided.

5.3 Power Supplies

Servers and communications equipment should be protected as far as is reasonable from the risk of power failure, power fluctuations or inadvertent disconnection.

5.4 Equipment Reliability

There should be adequate arrangements to facilitate the prompt repair or replacement of faulty equipment, and the Security Manager and/or System Manager should maintain a record of the various contracts in place.

6. Administrative Access Security

6.1 Access to the administrative functions associated with the practice system or network (user permissions; audit trails; backup procedures et), will be limited to authorised and suitably trained staff.

6.2 The System Manager as appropriate will ensure that there are adequate arrangements for the continuity of administrative access in the event that the person responsible should leave or passwords be forgotten.

6.3 Where systems are managed by a third party (EMIS or CSU) access should be re-established by liaison with the third party.

6.4 Where the Practice is solely responsible for system administration, administration IDs and passwords should be placed in a sealed envelope accessible to named individuals should the need arise.

6.5 Wherever possible, administrative functions should be operated through personal user IDs established for that purpose, rather than through default admin accounts provided with the system.

7. Control of Software Systems

7.1 The practice will not permit the installation of unlicensed software to any of its computers.
7.2 Software (including shareware and freeware) may be installed only with the approval of the security manager.
7.3 The Security Manager will maintain a record of software license purchases and renewals together with documentary evidence (purchase order/invoice/license certificate). Documentary evidence may not be required in some instances, and some may be held elsewhere.

8. Business Continuity Plans

8.1 The Security Manager / System manager will establish appropriate arrangements for the continuity of key business functions in the event of a failure in systems or communications.

8.2 Plans should cover:

- Back-up procedures to enable restoration of lost data
- Fall back arrangements for the loss of key hardware or communications
- Interim measures for the transfer of clinical messages normally processed electronically
- Interim (paper based) measures for recording of patient information, production of prescriptions etc.
- Recovery arrangements for the updating of systems from paper records when restored.

8.3 The practice will carry out an annual IM&T security risk assessment to evaluate the continued relevance and adequacy of the business continuity plan, and to identify and minimise other risks relating to IM&T security and confidentiality.

9. Security Incidents

9.1 The Security Manager will maintain a record of significant security incidents using the Non Clinical Incident process. The record will include:

- date time and location of incident
- how and by who the incident was discovered
- a description of the incident and its effect if any
- action taken to correct any effect
- measures taken to prevent or limit future incidents

9.2 The term “significant incident” is open to interpretation but should include any event leading to system downtime, loss or corruption of data, suspected intruder access, virus detection and any suspected malicious attempt to interfere with services or data. The Security Officer is responsible for determining whether or not an event constitutes a "significant incident", and for initiating any subsequent investigation.

9.3 The Security Officer will report "significant incidents" to the Senior Partner as appropriate. Where the incident involves a malicious action by a member of staff, the Security Officer will immediately disable that person's access privileges.

9.4 Any security incident impacting upon or likely to impact upon, NHSNet data, services or users is to be promptly reported to the CSU.

9.5 The security incident record should include incidents arising from the use of paper records.

10. User Guide

The Practice will provide further guidance to staff, explaining in more detail their responsibilities for security and confidentiality, and providing advice on security of the smart cards, password use and general good practice.

This will be done by a reading requirement request on our intranet of this policy for each staff member along with the practice policy on confidentiality. The security policy will become part of the induction pack for all new staff.