Data Security and Protection Policy

Introduction

The Data Protection Act 1998 (DPA) requires a clear direction on policy for security of information within the practice. The policy will provide direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information. The following is a Statement of Policy which will apply.

The Policy

- The practice is committed to security of patient and staff records.
- The practice will display a poster in the waiting room explaining to patients the practice policy (see below)
- The practice will make available a brochure on Access to Medical Records and Data Protection [*] for the information of patients.
- The practice will take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's consent, unless otherwise legally compliant. This will include training on confidentiality issues, DPA principles, working security procedures, and the application of best practice in the workplace.
- The practice will undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.
- The practice will maintain a system of "Significant Event Reporting" through a no-blame culture to capture and address incidents which threaten compliance.
- DPA issues will form part of the practice general procedures for the management of risk.
- Specific instructions will be documented within confidentiality and security instructions and will be promoted to all staff.

Partners

Responsibility for information security resides ultimately with the Partners.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is responsible for information risk within the practice and advises on the effectiveness of information risk management across the Organisation

.

Data Protection Officer (DPO)

The practice is required to appoint a Data Protection Officer by the General Data Protection Regulation (GDPR). The Information Governance Policy establishes this role. The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The DPO reports to the SIRO.

Practice Manager

The practice manager is responsible for the security of their physical environments where information is processed or stored. Furthermore, they are responsible for: Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area of work. Ensuring that all staff, permanent, temporary and contractor, are aware of their personal responsibilities for information security. Determining the level of access to be granted to specific individuals Ensuring staff have appropriate training for the systems they are using. Ensuring staff know how to access advice on information security matters

The practice manager will be responsible for maintaining appropriate policies and guidance for staff around the use and processing of personal data of information contained within the practice's information assets in line with data protection and data security legislation and regulations.

Camden GP IT

Camden GP IT is responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure NHS England's systems and infrastructure remain compliant with the Data Protection Act 2018.
It is also responsible for ensuring that all NHS England electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

Information Asset Owner

All Information Asset Owners (the practice manager with Camden GP IT) are responsible for ensuring that third party data processors have appropriate ISO and/ or Cyber Essentials accreditation where appropriate for assets stored electronically with third parties. Information Asset Owners are also responsible for ensuring appropriate data protection assurance from all third party suppliers processing NHS England data.

All Staff

All staff are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should undertake their mandatory annual Data Security Awareness training and understand:
• What information they are using, how it should be protectively handled, stored and transferred.
• What procedures, standards and protocols exist for the sharing of information with others.
• How to report a suspected beach of information security within the organisation.
• Their responsibility for raising any information security concerns with the practice manager.

Contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

Policy Framework

Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions and descriptions.

Security Control Assets

The practice will work with GPIT on an asset management process and associated system.

All ICT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

Access Controls

Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant IAO.

Computer Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

Application Access Controls

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

Equipment Security

In order to minimise loss of, or damage to, all assets, the Corporate ICT Team shall ensure that all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards.

Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with third party vendors working for and on behalf of the practice.

Information Risk Assessment

All information assets will be identified and assigned an Information Asset Owner (IAO). IAO's shall ensure that information risk assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). IAO's shall submit the risk assessment results and associated mitigation plans to the SIRO for review. Please see the Information Risk Procedures for further information.

Information Security Events and Weaknesses

All NHS England information security events, near misses, and suspected weaknesses are to be reported to the Head of Corporate ICT Technology & and Security or designated deputy and where appropriate reported as an Adverse Incident. All adverse incidents shall be reported to the DPO. The Information Security Incident Reporting procedures must be complied with.

Protection from Malicious Software

The organisation and its Corporate ICT service providers shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the practice manager. Users breaching this requirement may be subject to disciplinary action.

Removable Media

Corporate IT systems automatically encrypt removable media. Removable media that contain software require the approval of the practice manager before they may be used on practice systems. Users breaching this requirement may be subject to disciplinary action.

Monitoring System Access and Use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. The practice will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training) In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law.

Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks are used in accordance with Camden GP IT.

Business Continuity and Disaster Recovery Plans

The organisation will implement a business continuity management system (BCMS) that will be aligned to the international standard of best practice (ISO 22301:2012 – Societal security – Business continuity management systems - Requirements). Business Impact Analysis will be undertaken in all areas of the organisation. Business continuity plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO has a responsibility to ensure that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

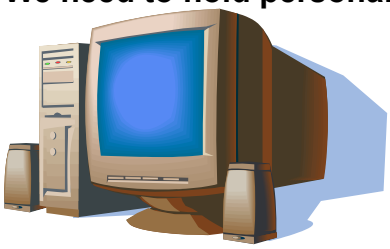
Training & Awareness

Data Security and Protection training is mandatory and all staff are required to complete annual on-line Data Security Awareness training.

PATIENT POSTER

DATA PROTECTION ACT – PATIENT INFORMATION

We need to hold personal information about you on our



computer system and in paper records to help us to look after your health needs, and your doctor is responsible for their accuracy and safe-keeping. Please help to keep your record up to date by informing us of any changes to your circumstances.

Doctors and staff in the practice have access to your medical records to enable them to do their jobs. From time to time information may be shared with others involved in your care if it is necessary. Anyone with access to your record is properly trained in confidentiality issues and is governed by both a legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safeguards are in place to prevent accidental loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example if a court order is presented, or in the case of public health issues. In other circumstances you may be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you. Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.

You have a right to see your records if you wish. Please ask at reception if you would like further details and our patient information leaflet. An appointment will be required.