South Manchester GP Federation Ltd

Bowland Medical Practice

Information Security Policy

Document name	Information Security Policy
Version:	0.1
Name of originator/author:	
Policy Owner:	
Date created	May 2018
Date reviewed	June 2018
Reviewer	
Date ratified:	
Ratified by:	
Next review date:	May 2019

Information Security Policy

1. Introduction

This policy has been designed to provide a framework of control and safeguards for the security of the information and systems used within Bowland Medical Practice.

A General Practice has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, other advisory groups to the NHS and guidance issued by professional bodies.

Information systems form a major part of the efficiency of a modern general practice. Adequate security procedures are critical in ensuring the Confidentiality, Integrity and Availability of these systems.

It is important that a general practice has an information security policy to provide management direction and support on matters of information security and confidentiality in general practice.

The Information systems used by the Bowland Medical Practice represent a considerable investment and are valuable assets to the Practice. The assets comprise equipment, software and data, essential to the effective and continuing operation of the Practice.

Much of the data is of a confidential nature, and it is necessary for all information systems to be protected against any events, accidental or malicious, which may put at risk the activities of the Practice or the investment in information.

This policy applies to all information systems used by, or for, the Practice. 'Information systems' include both computer-based systems and, non-computer-based systems. All staff are required to adhere to this policy.

This policy is in addition to the requirements specified within the NHSnet General Practice Code of Connection.

2. Purpose and Scope

The purpose of this policy is to protect, to a consistently high standard, all information assets. The policy covers security which can be applied through technology but also, it encompasses the behaviour of the people who manage information in the line of day to day practice business.

- To bring to the attention of all staff the need to improve and maintain security of information systems, and to advise managers of the approach being adopted to achieve the appropriate level of security.
- To bring to the attention of all managers and staff, their responsibilities under the requirements of relevant legislation, including Data Protection Act 2018 and Human Rights legislation and guidance, and the importance of ensuring the confidentiality of personal and sensitive data.
- To ensure that the Practice complies with current legislation and EU Directives, meets its statutory obligations and observes standards of good practice.
- To minimise the risk of security breach and prosecution.
- To meet the requirements for connection to the NHS network.

Information security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the practice is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff when working on practice business.
- A strengthened position in the event of any legal action that may be taken against the practice.
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

Scope

This policy is applicable to all surgery premises under the responsibility of the Partners and the information systems and data that can flow into or out of them.

3. Aim and Objectives:

The purpose of information systems security is to ensure an appropriate level of: -

Confidentiality: Information is obtained, held and disclosed lawfully and data access is confined to those with specified authority to view and/or change the data.

Integrity: Information shall be complete and accurate. All system assets and networks shall be operating correctly according to specification. This means that everyone involved is required to maintain the integrity of all the data within the practice by:

- Taking care over input
- Checking that the correct record is on the screen before updating
- Learning how the systems should be used and keeping up-to-date with changes which may affect how it works
- Reporting apparent errors to the Security lead (a nominated individual within the practice)

Availability: Systems and data are available when required and the output from it delivered to the right person, at the right time, when it is needed. This means a nominated member of staff is required to maintain the Availability of all the data by:

- Ensuring that the equipment is protected from security risks
- Ensuring that backups of the data are taken at regular intervals
- Ensuring that appropriate contingency is in place for equipment failure or theft and that these contingency plans are tested and kept up-to-date.

Objectives

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Practice:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation.
- Describing the principles of security and explaining how they shall be implemented in the practice. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the practice a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the practice

4. Roles and Responsibilities

4.1 GPs/Partners

GPs have overall responsibility for strategic and operational management, including ensuring that Bowland Medical Practice's policies comply with all legal, statutory and good practice guidance requirements.

GPs/Partners are responsible for ensuring that everybody employed by the Practice understands the need for, and maintains, information security. They also have overall responsibility for ensuring that systems and mechanisms to protect information security are in place. This means that each Practice must ensure:

- there is a named individual within the practice to be the nominated Security Lead.
- a suitable forum for security issues should be established within the practice.
- all staff have the opportunity and mechanism available to report security concerns.
- employee contracts contain confidentiality agreements.
- employee job descriptions detail security responsibilities.

- contracts with third party suppliers have appropriate clauses containing security and confidentiality requirements.
- a regular physical security check to assess whether adequate measures are in place should be undertaken.
- the staff and assets are secure and to prevent unauthorised access, damage and interference to the daily workings of the practice.

The Partners must endorse the requirements of this policy and encourage all staff to follow it.

4.2 The Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient identifiable information.

4.3 Practice Managers

Practice managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon.

They are also responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that information security is included in inductions for all staff.

They will determine the level of access to be granted to specific individuals and ensure staff know how to access advice on information security matters and monitor potential and actual security breaches.

They will act as a key contact to South Manchester GP Federation to co-ordinate any confidentiality breaches which may be a breach of the Data Protection Act 2018.

The Practice Manager must ensure that every member of staff, including staff who may only visit on a casual basis but require access to information or computer systems necessary to carry out their role, understands the principles within this policy. They must also work alongside IT Specialist Support, to ensure the correct function and security of the computing systems and granting access to approved users.

The Practice Manager will co-ordinate the training and development of staff to use the information systems in accordance with the necessary guidance and relevant legislation.

4.4 All Staff

All members of staff are required to preserve the security of the assets and information of the practice and bring any concerns that threaten this security to the attention of the Security lead.

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 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 Practice.
- Their responsibility for raising any information security concerns with the Practice Manager.

Contracts with external contractors that allow access to the Practice'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.

Each member of staff must be aware of his/her responsibilities when using information that is personal and be aware that it may only be used in accordance with the Data Protection Act 2018.

Staff must also be aware that clinical information within a general practice is governed by the Common Law Duty of Confidentiality and Caldicott good practice principles.

5. Policy Framework

a. 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.

b. Security Control of Assets and Risk Assessment

In order to make the best use of resources, it is important to ensure that each Information system is secured to a level appropriate to the measure of risk associated with it. A risk assessment should be carried out for each of the practice's information systems and measures put in place to ensure each system is secured to an appropriate level.

Responsibilities and procedures for the management and operation of all computers and networks should be established, documented and supported by appropriate operating instructions. 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.

It is important to ensure that all staff and assets are secure to prevent unauthorised access, damage and interference to the daily workings of the practice.

The practice must carry out a risk assessment which assesses whether adequate measures are in place. If adequate measures are not in place, appropriate action must be taken to reduce the level of risk.

Effective security measures are essential for protection against a risk of an event occurring, or to reduce the impact of such an event. Such events may be accidental or a deliberate act of sabotage.

A range of security measures can be deployed to address: -

- the Threat of something damaging the Confidentiality, Integrity or Availability of information held on systems or manual records
- the Impact that such a threat would have if it occurred
- the Chance of such a threat occurring

The Security lead at the Practice must consider the risks associated with the way in which the Practice works, the computer systems and the information that is held on them.

c. Computer systems

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. Where we engage with third parties to process personal data on Bowland Medical Practice's behalf, we stipulate our privacy expectations in written instructions. They are under a strict duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

In order to minimise loss of, or damage to, all assets, equipment shall be; identified, registered and physically protected from threats and environmental hazards.

General practice assets and equipment must not be removed from the premises or lent to anyone without the permission of a Partner or the Practice Manager.

Practice systems must only be used for approved purposes authorised by the Partners and managed by the Security lead.

Only suitably qualified or experienced staff should undertake maintenance work on, or make changes to, the practice systems.

Only authorised software may be installed and it must only be used in accordance with the software licence agreement.

Adequate documentation should be produced or made available for users as appropriate.

To maintain the integrity and availability of practice systems, backups of practice software and information must be taken regularly.

All information security incidents, near misses, and suspected weaknesses are to be reported to the Partner, Security Lead/Practice manager and Caldicott Guardian. Contact the South Manchester GP Federation lead to discuss if the incident needs further reporting e.g. as an "Adverse Incident".

Responsibility for the security of information assets must be assigned to a named individual known as the Information Asset Owner.

d. Passwords

Each individual is responsible for keeping their own password secure, and must ensure it is neither disclosed to nor used by anyone else, under any circumstances. Staff must only access systems using their own login and password. All staff are accountable for any activity carried out under their login and password, and this is audited.

Passwords must be adequate to provide the first line in defence to unauthorised access to data or systems.

Passwords should be a minimum of 8 characters in length with a mixture of letters and numbers and have an expiry date.

Passwords must be changed regularly.

e. Access Controls

Access is controlled on the basis of service requirements. Access to information shall be restricted to users who have an authorised business need to access the information and as approved by the relevant Information Asset Owner.

Access must be granted to, and revoked from, information systems in a controlled manner.

The user list must be reviewed regularly.

Leavers and those no longer requiring access for their duties must be removed from the system immediately.

Access to ICT facilities shall be restricted to authorised users who have a business need to use the facilities.

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 also depend on the availability of a license from the supplier.

f. Protection from malicious software

Unless completely isolated, computer systems are continually at risk from virus infection. Viruses may be received as:

- an e-mail message or as an attachment to a message
- a macro within a word or spreadsheet document
- an infected program that has been downloaded
- an addition to removable media e.g. CD's

The Practice 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 Practice's property without permission from the Security Lead. Users breaching this requirement may be subject to disciplinary action.

If a virus is suspected, prompt action is essential: inform the Security lead immediately.

g. Removable media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Security lead before they may be used on the Practice systems. Such media must also be fully virus checked before being used on the Practice's equipment. Users breaching this requirement may be subject to disciplinary action.

h. 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.

i. New information systems

The Practice shall ensure that all new information systems, applications and networks include a Data Protection Impact Assessment (see ICO guidance or contact the South Manchester GP Federation for advice) and are approved by the Security lead before they commence operation.

j. System Change control

Changes to information systems, applications or networks shall be reviewed and approved by the Security lead.

k. Business Continuity Management

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 Practice must ensure it has appropriate Business Continuity management arrangements for information assets that include but are not limited to answers to the following queries:

- Who would the police call "out-of-hours" if the alarm goes off? What about other emergencies discovered at your premises?
- Who are the key personnel who would need to be involved if an emergency occurs at the practice?

- Who is your Clinical IT System Supplier who would need to be involved if an emergency occurs at the practice?
- Ensure that your keyholder details with the police, local authorities (if applicable) or Alarm Company are up-to-date.
- Maintain a list in priority order of designated keyholders who may be contacted in the event of an emergency. Review and update this list regularly.
- Keep some torches in a handy location. Test them regularly and keep spare batteries. If re-chargeable, discharge regularly in accordance with the manufacturers recommendation.
- There are appropriate disaster recovery plans in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

i. Classification of Sensitive Information

The Practice shall implement appropriate information classifications controls, based upon guidance contained within the IG Toolkit to secure their information assets.

6. Monitoring

Compliance with this policy will be monitored via the Security Lead/Practice Manager, together with independent reviews on a periodic basis.

7. Training

Training will be provided to staff on induction and every 2 years to ensure they are aware of their confidentiality obligations in line with this policy.

8. Useful Links:

1. Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

2. General Medical Council's updated GDPR guide to confidentiality:

https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors#confidentiality

3. Article 8 of the Human Rights Act (1998) refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

http://www.legislation.gov.uk/ukpga/1998/42/contents

4. The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:
    - Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
    - Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
    - Unauthorised acts with the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

http://www.legislation.gov.uk/ukpga/1990/18/contents

5. The NHS Confidentiality Code of Practice (2003), updated Nov 2010, outlines for main requirements that must be met in order to provide patients with a confidential service:
    - Protect patient information.
    - Inform patients of how their information is used.
    - Allow patients to decide whether their information can be shared.
    - Look for improved ways to protect, inform and provide choice to patients

http://webarchive.nationalarchives.gov.uk/+/http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550