**BALMORAL SURGERY**

**Canada Road, Deal Kent CT14 7EQ**

**Tel: 01304 373444**

Manager: Mrs L Betts

Reviewed 23.01.20, 29.12.20, 31.05.22 31.05.23

# Balmoral Surgery Information Security and Confidentiality Policy

# Introduction

The Practice is aware that it 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.

This policy has been designed to provide a framework of control and safeguard for the security of the information and systems used within the practice

This policy will be reviewed annually.

**Purpose**

This policy sets out the high - level policy framework and principles adopted by Balmoral Surgery to govern information and confidentiality.

The practice recognises the need for an appropriate balance between openness and confidentiality and security in the management, storage and use of information, whilst recognising public accountability. The practice places significant importance on the confidentiality of, and the security arrangements required, to safeguard both personal information (staff and patients) and commercially sensitive information.

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

**Information Security comprises of;**

**Confidentiality**

* Everyone involved is required to maintain the Confidentiality of all data within the practice by:
* Ensuring that only authorised people can gain access to the information and systems
* Not disclosing information to anyone who has no right to know, see or be aware of it

**Integrity**

* 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 Information Governance Lead.

**Availability**

* The information governance lead 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

**Responsibility**

* A named individual within the practice has been nominated as Security Lead.
* All staff has the opportunity and mechanism available to report security concerns.
* Employee contracts contain confidentiality agreements.
* 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.

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

**Information Security is everyone’s responsibility**

The Practice Manager ensures 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 guide.

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

The Practice Manager should ensure that any notification required under the Data Protection Act 1998 is maintained and is current and kept up-to-date.

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 Practice Manager.

Each member of staff should 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 1998.

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

**Training**

Practice staff should receive adequate training to fulfil their role and understand their responsibilities within the practice.

Further training requirements must be reviewed regularly to ensure continued awareness and compliance with system developments, legislation and good practice.

All staff should receive information security and confidentiality training.

Patient Information

The practice should use patient-identifiable information only for the individual patient’s health care, for internal audit arrangements and to justify certain payments to the general practice.

(Under certain circumstances, visiting computer engineers may in the course of their work view patient-identifiable information. Such engineers must be bound by strict contractual agreements containing legal and confidentiality requirements.)

Data that has been anonymised such that patients cannot in any way be identified may be used by the practice and other clinical organisations for research purposes without seeking further consent.

Apart from disclosures required by law all other uses of information will require patient consent.

**Computer Systems**

Practice systems must only be used for approved purposes authorised by the Partners and managed by the Security lead, or if applicable, the IT specialist.

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, back-ups of practice software and information must be taken regularly.

If the internal network is connected to other services outside the practice, then additional care must be taken when using these services e.g. the NHSnet. The NHSnet (nww) is a private network for the NHS offering information and e-mail communications. If connected, access will be possible through this service to connect to the World Wide Web (www), commonly known as the Internet. This will enable the practice user to view (or browse) a whole range of ‘Web Sites’ and send e-mail communications around the world.

The NHSnet managed service provider (BT or Cable & Wireless) monitors the use of this network.

Any incident leading to a breach of security of the practice or information held within it must be reported to the Security lead.

**Passwords**

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

Passwords should be a minimum of 6-8 characters in length

with a mixture of letters and numbers and have an expiry date.

Passwords must be changed regularly.

**Access Control**

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.

**Anti Virus**

Unless completely isolated, computer systems are continually at risk from virus infection. This risk is greater as the volume of data transferred between systems and networks increases.

While most viruses are relatively harmless, they can cause serious disruption to both the user and the wider network.

Viruses may be received as:

* an e-mail message or as an attachment to a message
* a macro within a word processor or spreadsheet document
* an infected program that has been downloaded

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

An appropriate version of anti-virus software must be installed on practice machines and receive regular.

**Strategy for Security updates**

Operating system updates/patches are received through Windows Update and controlled/managed by the AEM (Autotask Endpoint Management) client installed on the PC.

PCs will check for updates every day at 11am via policies set up through AEM

**Transmitting Patient Data**

Some physical areas of the practice should be restricted and provide a ‘safe haven’ for the use and control of patient information.

It should not be assumed that other premises have the same level of security.

Good practice guidelines must be followed when sharing personal information. When sharing personal information by Post, Phone and when either Transporting or Disposing of personal information.

**Access and Equipment Monitoring**

The protection of assets is essential. Both software and hardware

Assets must be accounted for and a level of ‘ownership’ established.

Examples of assets associated with information systems are:

- Information & Data

- Software Programs

* Physical Equipment

e.g. practice server, desktop computers, printers and laptops

* Services

Responsibility for the security of information assets has been assigned to the Information Governance Lead, along with the CSU who own the hardware.

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.

**Mobile Computing**

Extra care must be taken when using laptops, tablets or mobile phones.

When connected to the practice through external telecommunications systems a secure level of authorisation and identity must be established.

These devices have an additional risk to their physical security from loss, theft or damage. Ensure that all serial number(s) of the equipment are written down.

Care must be taken to ensure that the data entered remotely is transferred as soon as possible to the practice system(s).

# Clear Desk Policy

The practice should ensure that all documents and information are removed from computer screens and desktops and are correctly filed when not in use.

# Disposal of Information & Equipment

Computer disks and equipment that contain personal data must have that information permanently deleted or destroyed.

**Note:** Re-formatting a disk or a computer ‘hard-drive’ does not guarantee that the information is deleted.

# Physical Safety & Security

The practice will work within the requirements of the relevant Health & Safety at Work Act to maintain a safe and secure environment for its employees, patients and visitors.

Safety and security systems installed on the premises must be operated in accordance with their instructions and should not be tampered with or repaired other than by suitably competent or qualified persons.

Electrical equipment must be used in accordance with the Electricity at Work Regulations.

Suspected defects must be reported to the Security lead as soon as possible.

All staff must have the opportunity and mechanism available to report security concerns.

# Risk Assessment

The practice recognises the importance of ensuring that all staff and assets are secure to prevent unauthorised access, damage and interference to the daily workings of the practice.

The practice should carry out a risk assessment which assesses whether adequate measures are in place

Where adequate measures are not in place, appropriate action should 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.

All staff should be aware of the threats, impact and possibilities of something damaging the Confidentiality, Integrity or Availability of information held on systems or manual records

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

###### All general practice staff are encouraged to consider the risks associated with the way in which they work, the computer systems and the information that is held on them.

# Incident Reporting

Any incident leading to a breach of security of the general practice or information held within it must be reported to the Practice Manager.

# Business Continuity Management

The practice has a documented business continuity plan in place. To limit the impact, in the event of an incident.