Dr. Rafaqat Rashid
MBChB, MA

Dr. Amar m. Bostan
MBChB, MRCP, MRCGP

PICTON MEDICAL CENTRE

http://www.pictonmedicalcentre.nhs.uk

Westbourne Green Community
Health Care Centre
50 Heaton Road
Bradford
West Yorkshire
BD8 8RA
Tel: (01274) 019605
Fax: (01274) 019610

Information Security Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1	28.1.2020	Rebekah Harrison	Anne-Marie Mitchel	

TABLE OF CONTENTS PAGE No.

STATEMENT

The security and protection of information is fundamental to the effective and efficient working of the practice and the maintenance of confidentiality.

This Policy provides a framework within which allows us to handle information and data in the most secure way, given the demands of the practice.

Security is everyone's responsibility and all personnel working in the practice must make every effort to comply with this Policy.

SCOPE OF POLICY

THE NEED

To meet legal and professional requirements and satisfy obligations to the NHS, the practice must use cost effective security measures to safeguard its information resources.

This Practice Security Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

THE POLICY

The Policy of the practice is to accept willingly all obligations in respect of information security and to protect its information resources by implementing recognised NHS best practices that will achieve a balance between cost and risk.

APPLICABILITY

The Policy shall apply to all partners and staff of the practice and any other healthcare professional using the IT resources of the practice.

IMPLEMENTATION

The requirements of the Policy shall be implemented by all partners, staff and other healthcare professionals using the practice's IT resources.

Any team member noting any area of conflict between this Policy and any other practice Policy must bring it to the attention of the **Practice Manager** as Security Officer of the practice, immediately for conflict resolution. **Dr A Bostan and Dr R Rashid and the Practice Manager** will in any case be responsible for the routine periodic review of the Policy.

Internal audit shall undertake independent reviews to assess the adequacy of implemented security measures including compliance with the Policy.

Compliance with the Policy is the duty of all partners and staff. In serious cases, failure to comply with the Policy may be a disciplinary matter and could also result in a breach of the law or a criminal offence.

Staff have an obligation to report suspected breaches of the Policy immediately to **the Practice Manager or Service Manager**
In the case of a breach or suspected breach that could affect the security of NHSnet, the **Practice or Service Manager** is to notify the CCG without delay.

INFORMATION RESOURCES

The Policy applies to all information whether spoken, written, printed or computer-based, which is owned, held in the custody of, or used by the practice.

The Policy also applies to all resources used in creating, processing, transmitting, storing, using or controlling that information.

OBJECTIVES OF THE POLICY

The objectives of the Policy are to ensure that:

- Information is protected from unauthorised access, disclosure, modification or loss.
- Information is authentic.
- Information and equipment are protected from accidental or malicious damage.
- Security risks are properly identified, assessed, recorded and managed.
- Safeguards to reduce risks are implemented at an acceptable cost.
- Audit records on the use of information are created and maintained as necessary.
- All legal, regulatory and contractual requirements and standards of due care are met.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy.

LEGAL OBLIGATIONS

GENERAL

The practice accepts its obligations to comply with the laws of the United Kingdom. All members of the team must be aware that there are legal requirements relating to information that must be met.

SOFTWARE COPYRIGHT

Software is protected by the Copyright, Designs and Patents Act 1988, which state that 'the owner of the copyright has the exclusive right to copy the work'.

It is illegal to make copies of software without the owner's permission. Penalties include unlimited fines and up to two year in prison.

COMPUTER MISUSE ACT

The Computer Misuse Act 1990 established three prosecutable offences against unauthorised access to any software or data held on any computer.

The offences are:

- Unauthorised Access to Computer Material
- Unauthorised Access with intent to commit or facilitate the commission of further offences
- Unauthorised Modification of Computer Material

KEY SECURITY CONTROLS

PERSONAL SECURITY

- **The Service Manager** and will ensure that all contracts of employment and any contracts of agency staff include a 'non-disclosure' clause.
- **The Service Manager** will ensure that security responsibilities are allocated to staff and written into job specifications and terms of reference.
- Security education and training will be provided to all staff as appropriate to their assessed needs.

PHYSICAL SECURITY CONTROL

1. Principle

Resources associated with information processing, such as offices, computer equipment, communications media and paper-based records shall be protected from unauthorised access, misuse, damage or theft.

2. Access

- The non-public areas of the practice premises are designated a secure area. Visitors are to be escorted at all times and a record of visits kept.
- In order to prevent unauthorised access during silent hours an alarm system is provided. Reaction to alarms and subsequent management action are detailed in the practice Health and Safety Policy.

3. Equipment Security

- All hardware and software assets held by the practice are to be held against a hardware register and be uniquely marked as being the property of the tPCT.
- No alteration to the hardware configuration of the system may take place without the permission of **Drs Bostan & Rashid and the Practice / Service Manager**. Under no circumstances are modems to be attached to any part of the system.
- On-going maintenance arrangements have been agreed with **Tpp SystmOne and Bradford & Airedale CCG**
- Only approved systems engineers and the Health Informatics Service Staff will be allowed access to hardware or software and such access are recorded.
- No remote diagnosis or repair services are permitted unless they are over NHSnet or the NHSnet connection is broken. All such diagnosis and repair is to be recorded.
- Computer hard discs are not to be removed from the practice premises without the written permission of the **Practice Manager** , **Service Manager of GP Partner**
- The disposal of any storage media is subject to specific security control. Simple deletion of files is not adequate and the advice of the CCG's Health Informatics Service is to be sought before any disposal.

INTERNAL SECURITY CONTROL

1. Principles

All information shall have an official owner who will be fully accountable for its protection and who will be responsible for:

- Assigning a security classification where appropriate.
- Defining who is authorised to access the information on a need-to-know basis.
- Assessing the risks to the security of the information and the impact of its loss, for both short and long periods.
- Employing suitable measures to reduce risks.
- Ensuring that equipment is only utilised for practice business.
- Ensuring that information is authentic, correct, complete and auditable.
- Ensuring that information is backed up regularly and at a frequency commensurate with its usage, and is validated in line with the recommendations laid out in the Application for 'Paperless' status.
- Safeguarding and retaining all practice records.
- Ensuring that information exchange with external organisations within or without the NHS does not compromise the confidentiality of sensitive information, nor does it increase the risk of data corruption.

2. Security Incidents and Reporting

A security incident is defined as any event that could result or has resulted in:

- The disclosure of confidential information to any unauthorised individual.
- The integrity of the system or data being put at risk.
- The availability of the system or information being put at risk.
- An adverse impact, for example:
  - Embarrassment to the practice, CCG and the NHS.
  - Threat to personal safety or privacy.
  - Legal obligation or penalty.
  - Financial loss.
  - Disruption of activities.
- All incidents or information indicating a suspected or actual breach of security must be reported immediately to **the Practice or Service Manager.** The types of incidents that can result in a breach of security are many and varied. Their severity will depend upon a myriad of factors but the majority will be innocent and unintentional and will not normally result in any form of disciplinary action. The likely result will be improved security and awareness throughout the practice.
- Any unusual incident must be reported to **the Practice or service manager who** will maintain a record of incidents.

  If an incident is considered to be significant, **the Practice or service Manager or GP Partner** is to be informed. Any incident where the security of NHSnet is at risk is to be notified to the Health Informatics Service (HIS) Information Governance Manager.
- Any member of staff reporting a breach of security will have unhindered access to **the Practice / Service Manager**.

  If that member believes the breach is as a result of an action or negligence on the part of **the Practice or Service Manager** then the member will have access direct to **CCG Health Informatics Service (HIS)**.

3. Virus Protection

- A computer virus is a computer program, which 'infects' (modifies or attaches itself to) other computer programs.

  It then replicates itself and when a set of conditions arises it performs its intended function. This can range from a silly message to the destruction of the complete data holding of a system.
- A constantly running anti-virus software package has been provided and where possible set to auto update latest virus signatures.

  This does not absolve users from specifically checking any externally sourced disc for viruses before downloading any data or application.

4. Passwords

Passwords are an effective security measure only if they are properly constructed and kept secret. Partners and staff will follow the following routines for password management.

All users should have an individual user name for logon.

- All passwords are to be changed on a regular basis through system forced password changes. Additionally, users are to change their password at any time that they feel their password has been compromised.
- Passwords should be given values that are not associated with personal characteristics, (e.g. children's names, telephone numbers, car registration numbers etc.)

  Simple and obvious strings of characters and numbers should not be used. It is recommended that a combination of alphabetic, numeric, upper and lower case and system characters be used.
- Passwords should not be written down except as possible reference by **the Practice/ Service Manager** under strict security control.
- Passwords are not to be revealed to or shared with other users.
- System passwords are to be maintained in hard copy form by the Security Officer and held in a sealed envelope under secure arrangements.

5. System Access Controls

No terminal of PC is to be left logged on and unattended. Users leaving their workstation are to log off the system, or change user, to prevent unauthorised access.

6. Housekeeping

- Data back up of the complete system will be done centrally of site, daily by **CCG Health Informatics Service (HIS)**. Users are responsible for the backup of data held on their PC hard disk.

  All backup data will be accorded the same level of security as live data and held separately at an off-site secure location.
- Removable magnetic storage media such as floppy disks and DAT tapes should be stored in a secure environment when not in use.
- All software in use by the practice must be licensed and networked applications may be subject to a limited number of users. **The Practice / Service Manager** is to ensure that software is correctly used against licences held.
- Software is not to be loaded onto any system or PC without the express authority of **the Practice / Service Manager & CCG Health Informatics Service (HIS)**. This Policy is also to be reflected in employee's terms and conditions of employment.

7. Service Continuity Planning

Disaster Recovery and Service Continuity Contingency plans are to be produced to ensure the continued fulfilment of the practice mission.

EXTERNAL SECURITY CONTROL

1. General

Any person not directly a member of the practice team is to be considered 'external'.

2. Information Exchange

The exchange of information with, and between, other organisations shall take place within formal arrangements that reflect the legal requirements and the sensitivity of the information.

3. NHSnet

- The NHSnet provides NHS wide networking facilities allowing the secure transmission of data and messages between NHS organisations that abide by the NHS Networking Security Policy.

  Implementation of that Policy and the NHS communal security undertakings detailed in the NHSnet Code of Connection have been accepted by the practice and copies are available in the library for information purposes.
- Throughout the NHSnet connection the practice has access to e-mail and EDI services (within and without the NHSnet), NHSweb and Internet World Wide Services.

  Users must note that the internet consists of uncontrolled, unmanaged and largely unsupported world-wide networks and is a source of much valuable information, not least in the area of Healthcare.

  However, it is also an unrestricted source of much illegal and illicit material. Additionally, it has a large recreational attraction.
- Whilst the access point to the Internet from NHSnet is by way of a secure gateway, once users have affected access to the Internet they are totally responsible for the management of the security aspects of their actions.
- Practice Policy for internet and e-mail use is as follows:
  - Internet and e-mail services outside NHSnet are available to staff for communication and research purposes.
  - No illicit or illegal material will be viewed / downloaded or obtained via the Internet or e-mail.
  - Any material downloaded must be virus checked immediately by the user.
  - The user will make their system available at any time for audit either by the **Practice / Service Manager and GP Partner**, the relevant Audit Authority or representatives of NHS Telecommunications Branch.
  - Breaches of security, abuse of service or non-compliance with the NHSnet code of connection may result in the withdrawal of all Internet services to the user.
  - Inappropriate use of the Internet will result in disciplinary action and may ultimately lead to dismissal. It may also be necessary to proceed with criminal charges depending on the nature of the incident.

ROLE OF THE PRACTICE SECURITY OFFICER

Anne Marie Mitchell, Practice Manager
Babra Mushtaq, Service Manager is the nominated Security Officer for the practice and shall:

- Under the direction of the **Practice Manager**, develop and manage the practice security programme.
- Develop issue and maintain the IT security strategy and Policy and agree them with the **Senior Partners**.
- Develop a strategic IT Disaster Recovery & Service Continuity Plan and advise the practice on its implementation.
- Create an information security awareness programme to include whole practice briefings, training and education.
- Provide information security consulting support to the practice.
- Investigate breaches of security and report findings and recommended action to the practice.
- Implement a compliance programme to evaluate the effectiveness of the information security programme.
- Report annually to the **Partners** on the effectiveness of the overall information security programme.

POLICY REVIEW

This Policy is to be reviewed on an annual basis by **the Practice Manager** to take account of changing circumstances, legislation, technology and security risks.

Any revisions to the Policy are to be approved by **the GP partner** prior to implementation.

STAFF COMPLIANCE AGREEMENT

All employed and attached staff must read this Policy and sign a certificate agreeing to abide by the requirements laid down in this Policy.

A specimen certificate is at Annex A overleaf.

Signed certificates are to be retained in a register maintained by **the Practice Manager**.

ANNEX A – STAFF COMPLIANCE AGREEMENT

Information Security Policy
-
Staff Compliance Agreement

I have read and understand
the Practice Information Security Policy
and agree to abide by the requirements laid down in the Policy.

Name	
Signature	
Date	

This Agreement is to be signed by all personnel working at
Picton Medical Practice
and is to be retained in the register maintained by
The Practice Manager