Guide for General Practice

Jai Medical Centre

Information Security
&
Confidentiality

Acknowledge: East Surrey Local Health Community

Purpose

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.

This guide has been designed to provide a framework of control and safeguards for the security of the information and systems used within general practice across East Surrey Local Health Community.

Where the practice is connected to the NHSnet, then this guide is in addition to the requirements specified within the NHS*net* General Practice Code of Connection[i]. A copy of this code is attached as Appendix 1.

Scope

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

Introduction

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.

Connection and access to the **NHSnet is conditional** on there being an Information Security Policy in place.

Wherever personal information is held, on paper or computer, it is subject to the eight Principles of the Data Protection Act 1998[ii].

Individuals and the practice may be prosecuted or subject to a claim for damages for any instance where the Data Protection Principles are breached or where a person suffers loss, damage or harm from misuse of information.

Applying this guide to normal working within the practice will greatly reduce the risk of loss, damage or misuse of information.

This guide should be communicated and available to all staff as appropriate.

Information Security comprises:

4.1 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

4.2 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 Security lead – *The General Manager.*

4.3 Availability

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

Organisation Responsibilities

- A named individual within the practice should be nominated as Security Lead.
- A suitable forum for security issues should be established within the practice.
- All staff must have the opportunity and mechanism available to report security concerns.
- Employee contracts must contain confidentiality agreements.

- Employee job descriptions must detail security responsibilities.

- Contracts with third party suppliers must 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.

Staff Responsibilities

Information Security is everybody's

Each practice must nominate a person to act as its Security lead.

6.1 Partners

- The Partners must endorse the requirements of this guide and encourage all staff to follow the guidance to the best of their ability.

6.2 Practice Manager

- 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 guide.

- 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.

- 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.

6.3 IT Specialist

- The IT Specialist, if appointed, is responsible for ensuring the correct function and security of the computing systems, and granting access to approved users.

6.4 Practice 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.

- 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 1998.

- 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.

Training

Practice staff must 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 at least annually.

Patient Information

Patients have a right to expect that information about them is kept confidential!

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.)

The Practice has produced a leaflet called "Your Information – What you need to know" for members of the public informing them how the NHS local health community uses their information. This leaflet should be displayed in prominent areas of the practice.

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. The NHS is working towards achieving Informed Consent where information is used for purposes other than stated above. Further guidance on when disclosures may be justified has been published by the General Medical Council (GMC)[iii].

Caldicott Report

The Caldicott Report on Protecting and Using Patient Information was produced in December 1997 and is mandatory within the NHS.

It developed a set of good practice principles against which every flow of patient-identifiable information should be regularly justified and tested.

9.1 Caldicott Principles

1. Justify the purpose(s) for using confidential information

2. Only use it when absolutely necessary

3. Use the minimum required

4. Access to confidential information should be on a strict need-to-know basis
5. Everyone must understand his/her responsibilities

6. Everyone must understand and comply with the law

A key part of the recommendations contained within the report was the establishment of a network of Caldicott Guardians of patient information; your Primary Care Trust has a nominated Guardian.

Caldicott Guardians have a responsibility to develop a framework of protocols to safeguard and govern the uses made of patient information within NHS organisations.

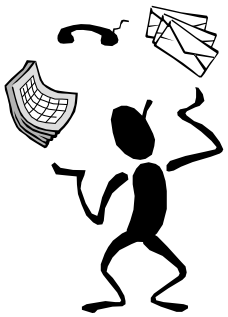
Any concerns relating to Caldicott should be made to the Security lead.

Caldicott Guardian Name: Suresh H Vaghela
Contact Details 07974954859

The practice must comply with all relevant legislation, including:

Data Protection Act 1998

This Act came into force on the 1st March 2000 and applies to information which relates to living individuals. The information may be processed by computer or held and stored manually in hard copy – for example as part of a 'structured' filing system (e.g. Lloyd George envelopes). Health records are specifically mentioned in the Act.



The practice must discharge its responsibilities under the Act including compliance with the eight Data Protection Principles: -

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for specified and lawful purpose(s) and not further processed in any manner incompatible with that purpose(s)
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data shall not be kept for longer than necessary
6. Personal data shall be processed in accordance with the rights of data subjects
7. Appropriate security measures shall be taken to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, the data
8. Personal data shall not be transferred outside of European Economic Area unless similarly protected

Note: The Data Protection Act 1984 required Registration every three years; under the 1998 Act Notification is required each year. **The General Manager** is required to ensure that Notification is adequate, current and kept up-to-date.

Notification information can be found on the Information Commissioner's website www.dataprotection.gov.uk. or for further advice contact Notification helpline on 01625 545 740.

DPA Notification Number: Z9327942

Expiry Date: 05th January 2025

Access to Health Records Act 1990[iv]

The Access to Health Records Act 1990 has been repealed, except in the case of records of the deceased.

Access to health records of living individuals is now governed by the Data Protection Act 1998, and there are no longer any date limits.

Subject Access Requests

Under the Data Protection Act 1998 any person has the right to request a copy of any information held about themselves. This is known as a 'Subject Access Request'.

A personal representative or any person who may have a claim arising out of the patient's death has a right of access to the relevant part of the deceased's health record.

- The practice must nominate a person to deal with Subject Access Requests.

- A general practice must have a written procedure for dealing with Subject Access Requests.

Appendix 2 details how to deal with an Informal Subject Access Request.
Appendix 3 provides a flow diagram for a Formal Subject Access Request Procedure.
Appendix 4 details a Formal Subject Access Request Procedure.
Appendices 5 – 13 contain forms which can be adapted by the practice to be used as part of a subject access request procedure.

Access to Medical Reports Act 1988[v]

This Act gives a right of access by individuals to reports relating to themselves provided by medical practitioners for employment or insurance purposes. This Act has not been superseded by the Data Protection Act 1998 and therefore remains in force.

Human Rights Act 1998[vi]

The Human Rights Act 1998, incorporating the European Convention of Human Rights, was adopted into UK law on 2nd October 2000.

It does not confer any new rights. The main difference is that individuals will be able to enforce the Convention in the UK courts, if they think a public authority* has breached or is likely to breach a Convention right or freedom affecting them. This may result in more challenges, well founded or otherwise.

The key Articles that relate to work within a general practice and the NHS include:

Article 2: *Right to life*
Article 3: *Right not to be subjected to inhuman or degrading treatment*
Article 5: *Right to liberty*
Article 8: *Right to respect for private and family life*
Article 9: *Freedom of thought, conscience and religion*

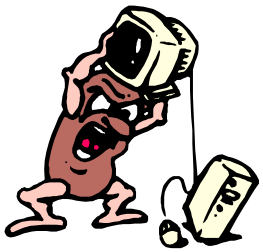
Article 12: Right to marry & found a family
Article 14: Prohibition of discrimination

A general practice must not act in any way that is incompatible with the Human Rights Act 1998.

*A general practice surgery carrying out work within the NHS is a public authority for the purposes of the Human Rights Act.

Computer Misuse Act 1990[vii]

This legislation created three criminal offences related to computer systems:



1. Unauthorised access
2. Unauthorised access with the intent to commit or facilitate the commission of further offences
3. Unauthorised modification

The Security lead should be notified immediately if there is a suspicion that any of these offences are, or may be, being committed.

Copyright, Designs and Patents Act 1988[viii]

This Act makes the use of un-licensed (pirated) software a criminal offence which could lead to fines and imprisonment.

Freedom of Information Act 2000[ix]

The Act gives a general right of access to information held by a public authority*. The Act requires each public authority to maintain a publication scheme listing information that will be published.

*A general practice surgery carrying out work within the NHS is a public authority for the purposes of the Freedom of Information Act.

Other Legislation

The following pieces of legislation or guidance are relevant or applicable to a General Practice, either as an employer or provider of health care (this list is not exhaustive):

- Common Law Duty of Confidentiality
- The Health and Safety at Work Act 1974 & 1992

- The Electricity at Work Regulations 1989
- The Health and Safety (Display Screen Equipment) Regulations 1992
- Manual Handling Operations Regulations 1992
- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
- 1995 (RIDDOR)
- Control of Substances Hazardous to Health Regulations 1988 (COSHH)
- Public Interest Disclosure Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Health and Social Care Act 2001

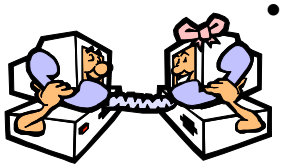
This matrix indicates how information relates to specific pieces of legislation or guidance.

	Common Law Duty of Confidentiality	Caldicott	Access to Health Records Act 1990	Computer Misuse Act 1990	Data Protection Act 1998	Human Rights Act 1998
Anonymised Information	NO	NO	NO	YES	NO	NO
Personal Information	YES	NO	NO	YES	YES	YES
Personal Health (Living)	YES	YES	NO	YES	YES	YES
Personal Health (Deceased)	YES	YES	YES	YES	NO	?

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 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, 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.

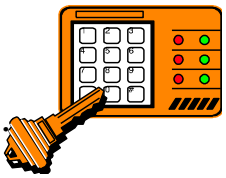
The NHSnet managed service provider (BT or Cable & Wireless) monitors the use of this network.

Connection to inappropriate sites on the Internet, downloading or sending offensive material may lead to investigation, disconnection and possibly prosecution!

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

19.1 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.

19.2 Access Control

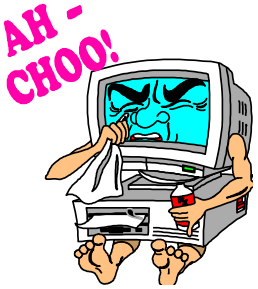
- Access must be granted to, and revoked from, information systems in a controlled manner.

- The user list must be reviewed regularly.

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

19.3 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.

Prevention is much more effective than the cure!

Computer diskettes or CD's must be scanned for viruses using approved anti-virus products.

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
- an addition to diskettes or CD's

- 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 updates of the 'engine' and antidote files (known as virus definition files).

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.

- Fax machines must only be used when absolutely necessary. If used, good practice guidelines must be adhered to. An example of a good practice guideline for faxing personal identifiable information can be found in Appendix 15.

- Good practice guidelines must be followed when sharing personal information. Appendices 16 – 19 provide guidelines when sharing personal information by Post, Phone and when either Transporting or Disposing of personal information.

The NHSnet and Internet are not secure for the transmission of personal or patient information without further protection such as encryption. This area is subject to a wider policy from the Department of Health and the British Medical Association.

Appendix 20 details guidance from the NHS Information Authority on how to use e-mail correctly.

Assets/Equipment Management

The protection of assets is essential. Both Software and Hardware assets must be accounted for and a level of 'ownership' established.

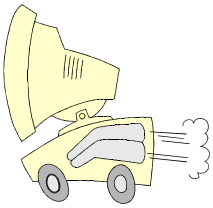
Examples of assets associated with information systems are:

- Information & Data
- Software Programs
- Physical Equipment
  e.g. practice server, desktop computers, printers and laptops
- Services

- Responsibility for the security of information assets must be assigned to a named individual.

- 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 laptop or palmtop computing devices.

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

This should be in accordance with NHSIA Acceptable Use Policy, Code of Connection, Appendix 1.

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.

- It is strongly advised that permanent security marking/engraving is used on all equipment.

- 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.

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

- Information containing personal details no longer required must be disposed of in accordance with the procedure in Appendix 19.

- 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

A general 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.

- A suitable forum for security issues should be available within the practice, for example, having an agenda item at regular meetings.

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

Risk Assessment

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.

- Each general 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

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 Security lead.

Business Continuity Management

Make preparations **NOW** – in the event of an incident its impact will be greatly reduced.

? 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.

28.1 Possible Incidents

- **Disruption or loss of data** (hard drive errors/theft of desktop machine)
- **Technology failures** (file corruption or network server failure)
- **Loss of skill-based services** (clinical software company/critical staff)
- **Local utility failures** (electricity/gas/water)
- **Communication Failures** (telephone/electronic)
- **Local incidents** (fire, flood, lighting strike, gas leak, burglary, criminal damage)

These are some examples of areas to be considered for incident management.

? Where would you meet if the building were unsafe?

Outside near the road, in the front and if the threat is in entrance area, we must meet at rear of the premises.

? Where could you conduct surgeries to see urgent patients?

Use the Contingency document.

? What method would you use to contact patients about the emergency arrangements?

Put a notice at the entrance, divert all calls to a number (Mobile or Land Line) which is manned continuously to give direction to patient

? How would patients make contact with the surgery during the disruption?

Either in person or by telephone.

? Where is the electricity consumer unit?

Outside at the entrance.

? Where is the gas isolation valve located?

In the gas boiler room

? Where is the water stopcock located?

Outside at the entrance

? What is the emergency telephone number for gas leaks?

British Gas 0800 111 999

? What is the telephone number of a local plumber?

Sunil the Plumber 07956685491

? What is the emergency telephone number for electrical faults?

Eastern Electricity 0800 783 8838

Notes:

[i] NHS*net* Security Network Connection Guide, Version 3.1 – 01/05/2001, Appendix F (Code of Connection to NHSnet for General Practices, Version 2.6)
[ii] Data Protection Act 1998 (Ch 29) – Act of the UK Parliament
[iii] General Medical Council - Confidentiality: Protecting and Providing Information
[iv] Access to Health Records Act 1990 (Ch 23) – Act of Parliament
[v] Access to Medical Report Act 1988 (Ch 28) – Act of Parliament
[vi] Human Rights Act 1998 (Ch 42) – Act of the UK Parliament
[vii] Computer Misuse Act 1990 (Ch 18) – Act of Parliament
[viii] Copyright, Patents and Design Act 1988 (Ch 48) – Act of Parliament
[ix] Freedom of Information Act 1990 (Ch 36) – Act of Parliament