Strand Medical

Quality Health Matters

# Information Governance

# Policy

| | |
|---|---|
| Policy number | CP 01 |
| Policy version | 1.5 |
| Category | Corporate |
| Originated | 01/01/2007 |
| Approved | 14/03/2011 |
| Reviewed | 21/02/2017 |
| Approved | 21/02/2017 |
| Review Date | 01/02/2018 |
| Reviewed | 26/11/2019 |
| Approved | 26/11/2019 |
| Next review due | 01/12/2020 |

## Index

1. Introduction .....5
1.1. About this policy .....5
1.2. Information security .....5
1.3. Types of Risks .....5
1.4. Types of Protection .....5
1.5. General Practice systems .....6
1.6. Roles within the Practice .....6
1.7. Assistance from outside .....7
2. Security Belongs to Everyone .....7
2.1. Introduction .....7
2.2. The information security policy .....7
2.3. Awareness .....7
2.4. Training .....7
2.5. Procedures .....8
2.6. Reporting of incidents and faults .....8
2.7. Personnel management .....9
2.7.1. Recruitment .....9
2.7.2. Existing personnel .....9
2.7.3. Leaving .....9
2.8. Security of the Practice .....9
2.8.1. Personal Safety .....9
3. Physical Protection .....10
3.1. What is Physical Protection .....10
3.2. Building Protection .....10
3.2.1. Secure Premises .....10
3.2.2. Building Design .....10
3.3. Preventing a break-in .....10
3.4. Preventing theft .....11
3.5. Maintenance .....11
3.6. Disposing the computer .....11
4. Protecting the data .....11
4.1. Introduction .....11
4.2. Back-up, storage and retrieval .....12

4.2.1. Back-up ....................12
4.3. What is archiving ....................12
4.4. Changes to software....................12
4.5. Virus protection....................12
4.5.1. What is a computer virus? ....................12
4.5.2. What is the effect of a virus? ....................12
4.5.3. How can I prevent a virus? ....................12
4.6. How to transfer information safely ....................13
4.7. Care of Printed material....................13
4.8. How to site and use computer screens....................13
5. Data Protection Impact Assessment (DPIA) ....................13
5.1. Contracts with data processors ....................14
5.2. Documentation ....................14
6. Remote Access ....................14
7. Unauthorised Access....................15
7.1. Keeping Data Confidential....................15
7.2. Access Control ....................15
7.3. Access Log ....................15
7.4. Means of Identification....................15
7.5. How to control passwords....................16
8. Networks....................16
8.1. What is a Network?....................16
8.2. The Dangers....................16
8.2.1. LANs....................16
8.2.2. WANs ....................16
8.3. Is the LAN safe? ....................17
8.4. Is the WAN safe?....................17
9. Business Continuity plan ....................18
10. Data Subject's Rights ....................18
10.1. Rights of individuals....................18
10.2. Consent ....................18
11. Caldicott Recommendations....................19
12. Legal requirements....................20
12.1. General Data Protection Regulations 2018 (GDPR)....................20
12.2. Data Protection Act 2018 (DPA18) ....................20

Appendix 1 - GDPR Organisational statement on Accountability ................................22
Appendix 2 - Procedure for Access Control..................................................................28
Appendix 3 - Responding to a Subject Access Request..............................................29
Appendix 4 – Procedure for Requests under the Freedom of Information Act ............33
Appendix 5 - Sharing information with other professionals..........................................34
Procedure for Access Control..........................................................................................35
Procedure for access to fax machines, servers, printers and care of printed material.36
Procedure for password choice and changing of password ........................................37
Procedure for log-on routines ..........................................................................................38
Procedure for maintenance, including remote maintenance........................................39
Procedure for prevention of intruders ..........................................................................40
Procedure for reporting of incidents and faults ............................................................41
Procedure for transferring information ........................................................................42
Procedure for virus protection.........................................................................................44

## 1. Introduction

### 1.1. About this policy

This policy provides guidance for all those working in the Strand Medical. It is used to promote security awareness amongst staff and provide patients/clients with the assurance that the surgery is providing adequate protection for the information they hold.

Information Governance comprises of the following areas:

- Information Management
- Information Technology
- Information Security
- Information - sharing protocols
- Legal requirements

Every member of staff must read this policy and ensure that they understand its contents and implications. Practice staff are asked to sign a statement confirming that they understand this.

Failure to comply with this policy may result in disciplinary procedures being instigated.

### 1.2. Information security

Information needs to be kept safe from loss, corruption, accidental or malicious breaches and unauthorised personnel. Information security aims to provide:

- Confidentiality – data access is confined to those with specified authority to view the data
- Integrity – all system assets are operating correctly according to specification and in the way the current user believes them to be operating
- Availability – information is delivered to the right person when it is needed
- Accountability – the ability to trace the actions of those using the system. For a paper record this will amount to a signature. In Electronic Patient Records this will include audit trails and appropriate authentication enabling the tracing/tracking and tying of record entries to individuals

### 1.3. Types of Risks

Systems can be subject to physical or logical threats.

Physical threats caused by natural disasters such as fire, flood, lightening or by the dangers of intrusion by unauthorized people.

Logical threats can occur when data are disclosed or altered in error or the software is changed in a detrimental way either accidentally or deliberately.

### 1.4. Types of Protection

Physical security measures include guarding the premises, providing adequate protection of the equipment and data and taking precautions in the event of fire, flood or burglary.

Logical protection means preventing unauthorized accesses by those inside and outside of the surgery, keeping data and software correct and preventing unauthorized changes.

### 1.5. General Practice systems

The Practice holds the following information:

- Patient information / records
- Staff information / records
- Company records

### 1.6. Roles within the Practice

The following roles have been established within the Practice:

| Role | Responsibilities |
|---|---|
| 1. Practice Business Manager | Oversees security, controls the budgets, ensures that confidentiality is maintained and that all staff members are appropriately trained.<br>Oversees the Reception Team and the smooth running of the Reception area. Ensures confidentiality is maintained at all times. |
| 2. Head of Nursing | Oversees the Nursing Team and ensures the appropriate use of their skills in the clinical environment. Also oversees that they are trained appropriately for their roles and their CPD is updated. Reports any significant events to the PBM. |
| 3. Deputy Practice Manager | Oversees the Administration team including Medical Secretaries. Ensures confidentiality is maintained at all times and reports any significant events to the PBM. |
| 4. Caldicott Guardian:<br>Dr Alistair McClumpha,<br>GP Partner | Overall responsibility for confidentiality and data security |
| 5. Information Governance Lead:<br>Kristina Svobodova,<br>Deputy Practice Manager | Day to day responsibility for the above |
| 6. Data Integrity Lead:<br>Dr Alistair McClumpha,<br>GP Partner | Responsible for the accuracy of the clinical data held |
| 7. Security Lead:<br>Kristina Svobodova,<br>Deputy Practice Manager | Responsible for systems access and passwords |
| 8. Data Protection Officer:<br>Dr Alistair McClumpha,<br>GP Partner | Responsible for overseeing compliance with the General Data Protection Regulations (GDPR) |

### 1.7. Assistance from outside

From time to time the Practice may require advice or assistance from others in the course of their work as follows:

| Role/Organisation | Type of Requests | Address/Tel/Fax/Email |
|---|---|---|
| North East London CSU | Support for IT hardware, software and communication problems | Tel: 0800 021 3337 or Self-service portal: https://marval.nelcsu.nhs.uk/NELSelfServiceLocal/Login.aspx?returnUrl=%2fNELselfservicelocal |
| SystmOne Help Desk | SystmOne-related software problems | 0113 205 0095 |

## 2. Security Belongs to Everyone

### 2.1. Introduction

Security belongs to everyone and every member of staff must follow the security procedures contained within this policy and report any possible breaches to the Practice Business Manager on ext. 5802.

The Practice Business Manager can also be contacted to discuss any security issues which may cause any member of staff concern.

Breaches in security are dealt with promptly and discussed with other members of the primary care team. Measures should be put into place to ensure that the breach of possible breach does not happen again. All breaches are reported as significant events within the Practice.

### 2.2. The information security policy

This policy emphasizes the importance of accurate, confidential and available data and the steps that are taken within the Practice to enforce and protect that data. The policy is available to all members of staff and can be located in \\h82011dc001\H82011-USF\~Emis-Shared-Folder\Management\Mgmt Shared\Policies\IGSOC. This policy should be updated whenever legislation or procedures change.

### 2.3. Awareness

Staff need to be aware of the need for information security. The practice provides training in security and confidentiality during induction and which continues throughout their working time at the Practice. All staff are given a copy of the Caldicott Principles as part of their induction and a copy of this Information Governance policy.

### 2.4. Training

Staff are given the opportunity and expected to attend any training offered by the CCG or IPC, other primary care training organizations (i.e. Syder & Young) or in house to ensure full understanding and compliance with security and confidentiality.
Information governance training is also available online from https://portal.e-lfh.org.uk/.

### 2.5. Procedures

Procedures are imperative as a first line of defence against security breaches. The following procedures have been developed and are a part of the IG Policy:

- Access control
- Access to fax machines, servers and printers and care of printed material
- Password choice and changing a password
- Log-on routines
- Flood precautions
- Maintenance, including remote maintenance
- Prevention of intruders
- Reporting of incidents and faults
- Responding to requests under GDPR, Access to Health Records Act and Freedom of Information Act
- Transferring information
- Virus prevention

### 2.6. Reporting of incidents and faults

Any incident (including ‘near misses’) or faults (even transient faults which appear to have righted themselves) which may lead to a breach of confidentiality or the integrity or availability of any data are reported to the Practice Business Manager or Deputy Practice Manager in his absence so that lessons can be learned and precautions taken against the same thing happening in the future.

Look out for:

- A stranger at the surgery premises
- Someone interfering with a PC
- A computer screen being observed by any un-authorised person
- Perceived fire risk
- Temporary loss of data
- Member of staff with authorised access looking at patient information not relevant to their job

Any such incident will be reported to a line manager or most senior person available as soon as possible.

The GDPR requires that certain types of personal data breaches are reported to the ICO. This will be actioned within 72 hours of becoming aware of the breach, where feasible. Breaches must be reported if they are likely to result in a high risk of adversely affecting individuals’ rights and freedoms. In these instances, as well as informing the ICO, the data subject(s) concerned will also be informed without undue delay.

The organisation has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not the organisation will need to notify the relevant supervisory authority and the affected individuals.

Additionally, a record will be kept of all personal data breaches, regardless of whether we are required to notify the ICO.

Please refer to the Practice’s Incident & accident policy for full details.

## 2.7. Personnel management

### 2.7.1. Recruitment

When recruiting staff (whether permanent, temporary or contracted) checks on past employment will be undertaken and candidates will be asked to explain any gaps in employment. References will always be asked for and followed up where appropriate to do so. All new staff members will be informed about information security as part of their induction.

All applicants for jobs at the organisation are informed that the data they provide as part of their application and possible future employment is used in line with data protection regulations.

On induction, new starters will read this policy and sign a confidentiality and information governance awareness agreement.

### 2.7.2. Existing personnel

All staff have a job description which clearly sets out the job they are to undertake, what data they are allowed to see and which they may change. Clinical system access is based on the ‘need to know’.

Contracts of employment will specify compliance with the Practice’s information security requirements and will contain a confidentiality clause, which will be explicit and include reference to disciplinary action where confidentiality is breached.

Deputies are appointed for all key members of staff as absences can make systems unavailable when required.

In order to ensure compliance with GDPR, all existing personnel will be advised of the Practice’s use of their data via a staff privacy notice and their rights in relation to their data.

### 2.7.3. Leaving

When staff leave they must immediately return all means of identification, e.g. keys, access passes, smart cards etc. and all passwords and access privileges are invalidated/withdrawn. Where staff have been dismissed or have walked out without notice, key codes e.g. burglar alarms, door codes are changed as soon as the member of staff leaves the building.

The leavers’ process is outlined for all line managers to follow, and can be found on the organisation’s shared drive.

## 2.8. Security of the Practice

### 2.8.1. Personal Safety

Fire Drill

The Practice has appointed the Head of Nursing and Deputy Practice Manager as Fire Officers. The Fire Officers should ensure that:

- Staff are told where the fire exits are
- Staff are aware of the assembly point outside the premises

- Staff are aware of the importance of closing windows and doors upon leaving the premises but not to the detriment of their safety
- Staff are advised, where safe to do so, to retrieve their Smartcards and lock computers upon leaving the premises
- That everyone gets out of the premises (role-call)
- All staff are aware of their responsibilities in case of fire
- Fire drills are carried out regularly
- Fire alarms are tested regularly
- Staff take fire safety training annually

The Fire Safety Policy can be found on the server in folder S:\~Emis-Shared-Folder\Shared\Policies\Health & Safety. This policy covers fire precautions and drill.

## 3. Physical *Protection*

### 3.1. What is Physical Protection

Physical protection or security means protecting the computer systems and the buildings in which they are held from physical harm, whether accidental or deliberate.

### 3.2. Building Protection

#### 3.2.1. Secure Premises

The premises are secured by alarm when not in use and the Practice has a Redcare contract if more than one alarm is activated. If only one alarm is activated, the Practice has a Key Holding contract with Banham to visit, check, secure the site and re-set alarms. There are window locks on all windows and appropriate door locks to comply with the Alarm contract. The premises have sufficient fire extinguishers, which are checked every 6 months by contracted company. Weekly fire alarm tests are carried out by the Office Administrator and one other allocated staff member.

Clinical file servers are stored in the server room that is not accessible to the general public.

#### 3.2.2. Building Design

At the premises used by the organisation there are security measures in place in order to prevent public access and to protect private areas.

There is no public access to staff areas and staff area doors have code locks on them. There is CCTV in situ to monitor the patient areas for anything suspicious and for health and safety. All clinical rooms have panic alarms and the panic alarm button is also part of the clinical system SystmOne.

Passageways are free of sensitive material (e.g. patient records) and expensive equipment. Computers and screens are placed away from patients to ensure security and confidentiality and ensure that there are no trailing computer/telephone wires to trip over.

All staff wear badges. Maintenance workers and visitors are issued with a visitor's badge and have to sign in and out of the visitors' book.

### 3.3. Preventing a break-in

Security Alarm and CCTV are in situ and advertised. Security lighting (PIF) is present outside all entrances.

All staff will remain vigilant, ensuring the doors to private areas are secured, external entrances are not left unlocked at the end of the day, and suspicious looking people are reported to a line manager or most senior member of staff on site.

### 3.4. Preventing theft

A fire proof safe is used for data and money. The safe is coded and only those needing to know are made aware of the code.

Staff should ensure personal belongings are not left where members of the public can access them.

The organisation keeps an inventory of all the equipment and software held including a full description of the model and the serial number of each unit – this can be found on the Information Asset Register.

Backups of data are done via back-up tapes provided by NEL CSU and clinical back-ups are provided by SystmOne.

High risk devices such as laptops have an encrypted hard drive and strong password protection system to prevent access to the data on a laptop in the event it is stolen.

### 3.5. Maintenance

All equipment and machinery require maintenance. Preventative maintenance will help prevent faults occurring. The organisation will ensure its equipment is covered by a maintenance contract, Service Level Agreement, or that maintenance is provided from the original supplier. Care will be taken with confidential information to ensure that no unauthorised accesses occur and that maintenance staff are covered by a confidentiality clause in their contracts. Contracts that the organisation holds with suppliers will be reviewed to reflect the responsibilities and liabilities of the suppliers in response to GDPR.

See separate Building Maintenance Policy v1.0.

### 3.6. Disposing the computer

Any disposal of NHSE IT equipment will only be considered with prior approval from the NEL CSU and NHSE will provide guidance on the process of doing so. The organisation will ensure that all data is removed when selling or disposing of computer equipment. Reformatting the hard disk does not destroy the data. The GP tech team can destroy hard drives. NEL CSU can be contacted for details of the company that can dispose of hardware under NHSE contract.

## 4. Protecting the data

### 4.1. Introduction

As well as providing physical protection it is also necessary to take precautions against data loss in the event of input errors, accidental loss, software errors, hardware failures, theft or corruption by taking backups and to know at what stage of data change those copies were taken.

## 4.2. Back-up, storage and retrieval

### 4.2.1. Back-up

The Clinical system is a web based national system which is backed up centrally.

Backing up of data on the practice server is carried out once daily to enable the practice to retrieve data in the event of a disaster, e.g. virus, data error, disc crash, theft, fire or flood.

If restore is needed in the event of a failure of some sort, the most recent copy of the backup will be used and any data entered after the last backup will be re-entered manually. From time to time backups should be tested by carrying out a full or partial ‘restore although if this is not possible attempts should be made to restore a fraction of the data to a spare area of disk in order to compare the two versions. NEL CSU will provide assistance.

## 4.3. What is archiving

Archiving is a process whereby data is copied to another medium not for the purpose of restoring data but to enable a permanent copy of the data to be kept for historical purpose. Archives should be subject to the same security as backups. Since the archive medium is subject to deterioration they should periodically be copied to new media.

## 4.4. Changes to software

Practice Business Manager or the Deputy Practice Manager will check with support services before making any changes or updating any software to ensure that it is compatible with existing software and use.
Software upgrades or new software will usually be provided and installed by the relevant software supplier. NEL CSU will provide advice and assistance as required.

## 4.5. Virus protection

### 4.5.1. What is a computer virus?

The dictionary definition of a virus is:

A program inserted without authorisation into a computer’s main program, which, when activated, interferes with the operation of the computer and of the computers with which it is linked.

### 4.5.2. What is the effect of a virus?

During the incubation period viruses will spread but will do no damage. When they are triggered they react in different ways. Some virus may change the held data or may delete files without the user realising. The virus will only infect programs but its damaging effect may reach any part of the data on hard disc, disk or connected server.

### 4.5.3. How can I prevent a virus?

These viruses can spread through file attachments in emails, the internet, or infected CDs, DVDs, memory sticks. All NHS organisations have a duty to install anti-virus software but infections will inevitably still occur.

The procedure for Virus Protection can be found at the Procedure for virus protection.

### 4.6. How to transfer information safely

If sensitive personal data needs to be transported to a different location the data should be:

- Encrypted if electronic
- Protected during transit by the use of a suitable transit case
- Delivered using a suitable carrier

The Safe Haven Policy is to be followed when transferring information by telephone, fax machine, post or taking paper-based person-identifiable information off site.

### 4.7. Care of Printed material

Computer printouts can carry extracts from the database, some of which will be confidential. Paper copies are more vulnerable than computer data because printed information can easily be read by most people.  Any such documentation is to be either stored securely out of reach of patients, or disposed of safely in the Shred-it bins when no longer needed. Shred-it bins are emptied monthly.

- Do not leave printouts lying around
- Site your printer so that passers-by cannot see confidential information being printed out
- Store confidential printouts securely, in locked cabinets and only removed when necessary by those authorized to do so
- Shred confidential printouts that are no longer required
- Lock prescription forms away when not in use

### 4.8. How to site and use computer screens

Computer screens should be placed where they cannot be easily over-looked and the user should ensure that confidential displays are kept to a minimum.  Screens should not be positioned facing windows or in the reception area where patients can see them.

If patients arrive with other members of the family or with a friend the screen should be shielded from the other people present.

## 5. Data Protection Impact Assessment (DPIA)

The DPIA process is the most efficient way for the organisation to meet its data protection obligations and the expectations of its data subjects. DPIAs are also commonly referred to as Privacy Impact Assessments or PIAs.

Following the implementation of the GDPR, a DPIA will be undertaken where:

- A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons; then the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
- Extensive processing activities are undertaken, including large-scale processing of personal and/or special data
- DPIAs are to include the following:
- A description of the process, including the purpose
- An evaluation of the need for the processing in relation to the purpose
- An assessment of the associated risks to the data subjects

- Existing measures to mitigate and control the risk(s)
- Evidence of compliance in relation to risk control

It is likely that these would be conducted in partnership with a data processor, in the instances that a new technology is being considered. (For example, an app to support the self-care of diabetes)

For further guidance on completing a DPIA, please refer to the ICO's website.

### 5.1. Contracts with data processors

The organisation as a data controller is liable for our compliance with the GDPR and will only appoint processors that can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. The organisation will use a processor who adheres to an approved code of conduct or certification scheme.

All data processors the organisation hold a contract with will be written to in order to seek assurance of compliance with the responsibilities and liabilities for data processors under GDPR. Further advice is awaited from the Information Commissioner's Officer as to how these responsibilities should be reflected should in these contracts. Following this further guidance, contracts will be revised.

### 5.2. Documentation

Data mapping is a means of determining the information flow throughout an organisation. Understanding the why, who, what, when and where of the information pathway will enable the organisation to undertake a thorough assessment of the risks associated with current data processes.

Effective data mapping will identify what data is being processed, the format of the data, how it is being transferred, if the data is being shared, and where it is stored (including off-site storage).

Alongside the organisation's data flow mapping, an information asset register will be maintained.

## 6. Remote Access

Members of staff may have remote access to the clinical system. This is protected by access to the secure NHS N3 network via a Virtual Private Network (VPN) protected with two factor authentication. Holders of VPN tokens will ensure these are kept in a safe place at all times and will not divulge their passwords to any unauthorized personnel. Remote access will only be used to complete clinical or business admin work.

# 7. Unauthorised Access

## 7.1. Keeping Data Confidential

The Practice computer holds staff details which are highly confidential but information about patients is ever more sensitive. You must take precautions to protect that information from:

- Staff members or patients that show too much curiosity
- Hackers who will use the telephone line or email communication to initiate their attack

Passwords must never be shared. Staff found sharing passwords or accessing another users account may be subject to disciplinary procedures. It is noted that clinical systems hold an audit trail. Any information entered under a user's ID will be treated as having been entered by that user and they are responsible for the data entered, changed or deleted.

Third party contractors may be employed by Practices from time to time e.g. builders, decorators, technicians etc. These must be subject to the same confidentiality clauses as employed staff. Contracted personnel should be asked to sign a confidentiality agreement.

## 7.2. Access Control

In order to identify who accesses information on the computer system every user will need to be issued with a username and password. Access rights need to be initiated to ensure that only those authorised to see information can have access to it.

The IG Lead within the Practice ensures that adequate controls are in place for issuing, validating, changing and withdrawing passwords and checks from time to time that access controls are functioning correctly.

The Procedure for Access Control can be found at Appendix 2.

## 7.3. Access Log

The computer system keeps a record of every attempt made to use it. The log records who has accessed the system, who has tried to access the system and been refused or those authorised users attempting to access information which they are not allowed to see.

After a certain number of attempts to log-on to a system (as determined by the system) the software will refuse to allow further attempts. The Access Log records these failed attempts.

Any misuse will be investigated. Users are made aware that any unauthorized access to any computer system may result in prosecution under the Computer Misuse Act 1990.

## 7.4. Means of Identification

Your password provides the means of identification. As you logon to your system your password will be authenticated before allowing you access. Users will be made to change their passwords every 3 months in order to log on to their PC and maintain security.

The password for logging on to the network will be changed regularly and a different password will be used each time it is changed.

Users will also change their password if they suspected that there has been a breach of security.

Any programs or software that have been authorized and are set up with a trial password will have a new password set as soon as possible.

### 7.5. How to control passwords

Passwords provide a means of determining who can access information. Passwords are the first line of defence to gaining access to an information system. However, passwords can be guessed or shared or hackers can use software to break a password if not that password is not well chosen.

The sharing of passwords is forbidden. Anyone found to be sharing password may be subject to disciplinary action.

Do not write your password down. A clue may be written and stored off-site.

## 8. Networks

### 8.1. What is a Network?

A network is a means of communicating between several points that are geographically separated. In this security policy we are concerned with Information Technology and networks that transfer data. The telephone network can be used for sending fax or data messages. Your Practice may have several direct links to other parties installed.

Systems that connect separate premises across a distance are known as Wide Area Networks or WANs. Systems that share data purely within the Practice are known as a Local Area Networks or LANs.

Whether WANs or LANs physical security of a network can be difficult to maintain and greater reliance must be placed on the logical precautions, such as verifying the authenticity of each message and controlling access to the data inside the computer system.

### 8.2. The Dangers

Four conditions to be avoided:

i. Sending confidential information to the wrong place
ii. Sending information to a place that is not well protected
iii. Receiving incorrect or misleading information from an unauthorised source and believing it to be correct
iv. A person using the network without authority to gain access to confidential data

#### 8.2.1. LANs

- Inappropriate or unauthorised access
- Careless use of or shared passwords
- Unsuitable placement of computer screens
- Users leaving computers active whilst leaving the room
- Unsecured servers

#### 8.2.2. WANs

- Control limited to what can be done at the ends of the network e.g. within the Practice
- Threats can affect available e.g. power failure at either end
- Messages misrouted; they may never arrive or go to the wrong people
- Dialling the wrong number

- Electromagnetic interference may destroy the integrity of the data
- Eavesdropping (tapping into a phone line)
- Unsecured servers

### 8.3. Is the LAN safe?

LANs are more easily defended than WANs because physical inspection is easily arranged.

- Servers within the Practice should be sited in locked rooms with key pad access and only accessible to authorised members of staff
- Exposed lengths of cables should be avoided to prevent people tripping over them
- Cables should be housed in conduits for added protection
- Fixing conduits at eye level will deter anyone thinking of tapping into the cables
- Consider confidentiality when setting up shared printers
- Printers and fax machines should be sited in ‘safe havens’ – locked rooms where only those authorised to access them can
- Printed material should be picked up promptly and not left on the printer or fax machine
- Be careful when placing PCs, do not site near a window that can be opened

Risks:

- Sharing introduces greater risk of loss of confidentiality
- Users losing work kept on their PC’s hard drive – these files must be backed up by the user themselves
- Spoofing – a user sending a message that looks as though it came from another user

Benefits:

- Central repositories of data can be easily be backed up by means of a single backup
- Users can log on to any PC and still be able to access their files

### 8.4. Is the WAN safe?

Once information leaves the premises it is completely out of the Practice’s control. You must, therefore, validate incoming messages and check on the recipient of messages you send out to ensure that you are only contacting authorised people and only receive genuine messages.

## 9. Business Continuity plan

The Practice has a set of documented procedures by which a site may hope to:

- Recover the use and availability of its Information Systems in the event of a catastrophe, as soon as is practically possible,
- Continue to operate to the optimum, while information systems are unavailable.

See Business Continuity Plan Policy.

## 10. Data Subject's Rights

### 10.1. Rights of individuals

The organisation will ensure that data subjects' rights are respected. Data subjects have a right to:

- Right to be informed;
- Right to access (See appendix 3 for Subject Access Request process);
- Right to rectification;
- Right to erasure (where engaged);
- Right to restrict processing;
- Portability (where lawful basis for automated processing is consent and processing is automated);
- Right to object;
- Right to object to automated decision making.

The organisation's privacy notices outline the lawful basis for which data is processed and data subject's rights in relation to these (rights available to individuals vary dependent on lawful basis- increased rights are available when the lawful basis relied on is consent.)

### 10.2. Consent

Relying on consent as the lawful basis for data processing is one way to comply with the GDPR, but it is not the only way. Consent is only appropriate where there is a genuine choice available not to consent. Most of our services will be based on providing a direct care service to patients and data handling is necessary for this purpose. In many health and social care contexts obtaining GDPR compliant consent will not be necessary and an alternative legal basis will be relied upon. Where this is the case, the organisation will not need to change its current consent practices, as long as they meet confidentiality requirements. (This will be documented within our privacy notice to patients. Please refer to GMC guidance for further information.

[1] https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality

[2] https://www.gmc-uk.org/ethical-guidance/learning-materials/understanding-the-new-data-protection-law

Following the implementation of GDPR, the organisation will ensure that the use of personal confidential data for any purposes other than direct care (e.g. for newsletter communications) will only be done so where an individual explicitly consents, and there will be a clear and easy process implemented for patients to withdraw this consent.

8.3 National Data Opt out

A new model for opting out of patient data being shared for research and planning purposes will be implemented. Patients will be informed that their information will be shared for their direct care. They will be given the option to opt out of their information being shared for research purposes or planning. However, where their data is pseudonymised /anonymised they cannot opt out. Additionally, if their data must be shared for legal reasons, they have no right to opt out.

Further guidance is awaited on this.

## 11. Caldicott Recommendations

The general conclusion of Caldicott was that data flows in the NHS were justified, but that in a number of instances the information was felt to be excessive for the purpose. A number of principles and recommendations were made.

Caldicott Guardian should be a GP or Practice Business Manager supported by a GP. The Caldicott Guardian should have the authority and be able to influence Practice policy and change working Practices if necessary.

The Practice Caldicott Guardian is Dr Alistair McClumpha.

**Principle 1 - Justify purposes(s)** – Individuals, departments and organisations must justify the purpose(s) for which information is required. This includes justifying the purposes to the public for specific patients as well as to the Caldicott Guardians within each organisation. Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian within the Practice.

**Principle 2 - Don't use patient-identifiable information unless it is absolutely necessary**
This means assessing information flows and uses and ensuring that patient identifiable information is removed unless a genuine case can be made for its inclusion and there is no alternative.

**Principle 3 – Use the minimum necessary patient-identifiable information** – Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably. This includes the use of the NHS number rather than any other identifier where possible.

**Principle 4 - Access to patient-identifiable information should be on a strict need to know basis** – Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see.

**Principle 5 – Everyone will be aware of their responsibilities** – Action will be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff are aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6 - Understand and comply with the law** – Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements. The most relevant and important of which are the Data Protection Act 2018, The Access to Medical Reports Act 1988 and the Police and Criminal Evidence Act 1984.

**Principle 7- The duty to share information can be as important as the duty to protect patient confidentiality** - Professionals should in the patient's interest share information within this framework. Official policies should support them doing so.

Every use of patient-identifiable information must be lawful.

Further information regarding Caldicott can be found on http://www.connectingforhealth.nhs.uk/infogov/resources/

## 12. Legal requirements

There are several acts of parliament that must be considered:

1. General Data Protection Regulation 2018 / Data Protection Act 2018
2. Human Rights Act 1998
3. Freedom of Information Act 2000
4. Crime and Disorder Act 1998
5. The Computer Misuse Act 1990
6. Copyright, Designs and Patents Act 1988
7. Access to Health Records Act 1990
8. Access to Medical Reports Act 1998
9. The Caldicott Guardian Manual (2017)
10. Confidentiality: NHS Code of Practice (2014)
11. The Records Management Code of Practice: Parts 1 & 2 (2016)
12. Confidentiality: good practice in handling patient information (GMC)

### 12.1. General Data Protection Regulations 2018 (GDPR)

The organisation has a responsibility to adhere to the principles of the General Data Protections Regulations and will demonstrate compliance by implementing the following measures. Key areas included within this to support compliance are:

- Contracts
- Documentation (Data flow mapping and Information Asset registers)
- Data protection by design and default
- The data protection officer
- Information Security, including physical security, cybersecurity, personal data breaches, staff awareness and training
- Retention

The organisation’s statement with regards to compliance with the GDPR can be found at Appendix 1.

### 12.2. Data Protection Act 2018 (DPA18)

All of the organisation’s staff will be made aware of the Data protection Act 2018 during their induction training and ongoing annual statutory training.

In addition to these two key pieces of legislation, a number of other legal requirements are relevant:

- Human Rights Act 1998
- Freedom of Information Act 2000Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- The Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1998
- Access to Health Records Act 1990
- Access to Medical Reports Act 1998
- NHS Guidance

## Appendix 1 - GDPR Organisational statement on Accountability

### 1. Summary

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

### 2. General Data Protection Regulations (GDPR)

Strand Medical Group recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The organisation fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The organisation also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The organisation believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

The Organisation is aware of and will adhere to the **General Data Protection Regulations (GDPR)**

Article 5 of the GDPR states that ***"the controller shall be responsible for, and be able to demonstrate, compliance with the principles." and that 'Personal data shall be***

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

The organisation has a responsibility to adhere to the principles of the General Data Protections Regulations and will demonstrate compliance by implementing the following measures:

Contracts
Documentation
Data protection by design and default
The data protection officer
Information Security, including physical security, cybersecurity, personal data breaches, staff awareness and training
Retention

## 3. Contracts

The organisation as a data controller are liable for our compliance with the GDPR and will only appoint processors that can provide ‘sufficient guarantees’ that the requirements of the GDPR will be met and the rights of data subjects protected. We will use a processor who adheres to an approved code of conduct or certification scheme.

Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don’t comply.

Contracts will be revised to reflect the responsibilities and liabilities when GDPR comes into law. The revised contracts will include a standard clause as provided by the ICO. In addition to this the contract will specify that the data processor in question will:

- The processor will only act on the written instructions of the controller;
- Ensure that people processing the data are subject to a duty of confidence;
- Take appropriate measures to ensure the security of processing;
- Only engage sub-processors with the prior consent of the controller and under a written contract;
- Assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- Assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- Delete or return all personal data to the controller as requested at the end of the contract; and
- Submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

## 4. Responsibilities of the Data processor

A processor must only act on the documented instructions of a controller. If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.

In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorization of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

If a processor fails to meet any of these obligations, or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor's obligations.

## 5. Documentation*/Data Flow Mapping*

The organisation will comply with GDPR article 30(1) and will document in writing and maintain a record of our processing activities, covering areas such as processing purposes, data sharing and retention.

This will include

- A description of the categories of individuals and categories of personal data. The name and contact details of our organisation (and where applicable, of other controllers, our representative and the data protection officer).
- The purposes of our processing.
- The categories of recipients of personal data.
- Details of our transfers to third countries (if any) including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of our technical and organisational security measures.

This will include information that feeds into our 'Privacy notice' such as

- the lawful basis for the processing
- the legitimate interests for the processing
- individuals' rights
- the existence of automated decision-making, including profiling
- the source of the personal data;

The rights available to individuals

- the right to be informed
- right of access
- right to rectification
- right to erasure
- right to restrict processing

- right to portability
- right to object
- rights related to automated decision making including profiling

And additional information to comply with transparency

- Controller-processor contracts;
- The location of personal data;
- Data Protection Impact Assessment reports;
- Records of personal data breaches;
- Information required for processing special category data or criminal conviction and offence data under the Data Protection Bill, covering:
- The condition for processing in the Data Protection Bill
- The lawful basis for the processing in the GDPR
- Our retention and erasure policy document.

## 6. Data protection by Design and default

Under the GDPR, we have a general obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

Privacy by design has always been an implicit requirement of data protection that the ICO has consistently championed.

We will ensure that privacy and data protection is a key consideration in the early stages of any project that is “likely to result in a high risk” and then throughout its lifecycle. For example when:

- Building new IT systems for storing or accessing personal data;
- Developing legislation, policy or strategies that have privacy implications;
- Embarking on a data sharing initiative; or
- Using data for new purposes.

The organisation will, when embarking on any of the above will complete the Data Protection Privacy assessment template supplied by the Information Commissioners office. Advice will be sought from the Data protection officer who will be informed at the start of the project the findings of which will be documented and will feed directly into asset registers/Documentation

## 7. Data Protection Officer (DPO)

The organisation is a ‘public authority’ for the purposes of the ‘Freedom of Information act 2000’ and GDPR. Our core activities mean we process special categories of data (health data). For that reason we appoint a data protection officer

Our Data Protection officer is Dr Alistair McClumpha.

The role of the DPO is;

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;

- To advise on, and to monitor, data protection impact assessments;
- To cooperate with the supervisory authority; and
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

The DPO will be involved, closely and in a timely manner, in all data protection matters, and will report to the highest level of management of the organisation.

The GDPR requires the organisation to publish the contact details of our DPO via our Privacy notice and provide them to the ICO. This is to enable individuals, and employees and the ICO to contact the DPO as needed.

## 8. Codes of conduct and certification

The organisation will adhere to any codes of conduct or certification scheme that become available that cover our processing activity. Adhering to these codes of conduct and certification schemes will demonstrate with:

- Improve transparency and accountability - enabling individuals to distinguish the organisations that meet the requirements of the law and they can trust with their personal data.
- Provide mitigation against enforcement action; and
- Improve standards by establishing best practice.
- When contracting work to third parties, including processors, we will consider whether they have signed up to codes of conduct or certification mechanisms.

## 9. Information Security

The organisation will establish and maintain policies for the effective and secure management of its information assets and resources.

- The Organisation will undertake or commission annual assessments and audits of its information and IT security arrangements.
- We undertake an analysis of the risks presented by our processing, by completing the **Data Security and Protection Toolkit** and use this to assess the appropriate level of security we need to put in place.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- The Organisation will promote effective confidentiality and security practice to its staff through policies, procedures and training.
- The Organisation will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- We will report personal data breaches to the ICO within 72 hours of being aware of them, where appropriate.
- We will use encryption and/or pseudonymisation where it is appropriate to do so.

When considering physical security, the Organisation will take into account:

- the quality of doors and locks, and the protection of our premises by such means as alarms, security lighting or CCTV;
- how we control access to your premises, and how visitors are supervised;
- how we dispose of any paper and electronic waste; and

- how we keep IT equipment, particularly mobile devices, secure.

When considering cybersecurity, the Organisation will take into account:

- system security – the security of our network and information systems, including those which process personal data;
- data security – the security of the data we hold within our systems, e.g. ensuring appropriate access controls are in place and that data is held securely;
- online security – e.g. the security of our website and any other online service or application that we use; and
- device security – including policies on Bring-your-own-Device (BYOD)

## 10. Personal Data Breaches

The organisation will report certain types of personal data breaches to the relevant supervisory authority. We will do this within 72 hours of becoming aware of the breach, where feasible.

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we will also inform those individuals without undue delay.
- We will ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we will need to notify the relevant supervisory authority and the affected individuals.
- We will also keep a record of any personal data breaches, regardless of whether we are required to notify.

## 11. Staff awareness and training

The GDPR requires that when acting under our authority with access to personal data staff will not process that data unless we have instructed them to do so. It is therefore vital that our staff understand the importance of protecting personal data, and are familiar with our security policy and put its procedures into practice.

The organisation provides appropriate initial and refresher training either online, internally or will commission appropriate training, which will enable staff so that;

- They have knowledge on our responsibilities as a data controller under the GDPR;
- They know and understand their staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- They are informed of the correct procedures to identify callers;
- They are made aware of the dangers of people trying to obtain personal data by deception (e.g. by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading our staff to alter information when they should not do so; and
- They are aware of and observe any restrictions you place on the personal use of your systems by staff (e.g. to avoid virus infection or hey spam).

## 12. Retention Policies

Information relating to individuals and staff will be held in accordance with the NHS Records Management Code of Practice for Health and Social Care 2016.

## Appendix 2 - Procedure for Access Control

1. The Security Lead or deputy will establish who needs access to the computer systems within the organisation
2. The Security Lead or deputy will decide what access level is required. The privileges accorded to each user will depend on their status within the service, their role and responsibilities. These privileges may be changed if a user's role changes and access withdrawn immediately if a user leaves the company.
3. The Security Lead or deputy will provide the user with a unique username and password for each system they need to use. In the case of clinical IT systems correct smartcard access profile. Local and NHS smartcard policies will be adhered to.
4. The user must immediately log on and change their password to something of their choice. This password must not be shared or used to allow anyone else access to the computer system.
5. The user can change their password at any time and will do so if they suspect others may know.
6. A user may be required to use other unique identifiers to gain access to other information systems.

Further information in Procedure for Access Control.

## Appendix 3 - Responding to a Subject Access Request

Patients have a legal right to see and be provided with a copy of their medical record. This is referred to as a subject access request. This right extends to the records of living individuals (see below for deceased patients).

The organisation's subject access request process has been reviewed in order to comply with changes outlined in GDPR 2018. Please note that this process may be updated, as further guidance is awaited.

### 1. Data Subjects' Rights

All data subjects have a right to access their data and any supplementary information held by the organisation. Data subjects have a right to receive:

- Confirmation that their data is being processed
- Access to their personal data
- Access to any other supplementary information held about them

The purpose for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them.

The process that the organisation shall follow for Subject Access Requests is detailed below:

a. Ensure the request is made in writing by the patient – this can be via letter or electronically (organisations should make available the ability to submit a request electronically.)
b. Ensure the request is passed directly to the manager responsible for SARs.
c. Upon receiving the request, the data controller must ensure that ID verification is requested and this should be stated in the response to the data subject upon receipt of the access request
d. Ensure all health records requests are dealt with within 28 days (previous subject access requests had a response time of 40 days).
e. In the case of complex or multiple requests, the data controller may extend the response time by a period of two months. In such instances, the data subject must be informed and the reasons for the delay explained.
f. If the request is made by a third party on behalf of the patient, ensure the patient has consented. The responsibility for providing the required authority rests with the third party and is usually in the form of a written statement or consent form, signed by the data subject. (Also see third party requests below to ensure request can be made as a SAR and not under AMRA)
g. A person with parental responsibility has the right to apply for access to a child's health record (see guidance for further information)
h. If the person providing the information is not a health professional, the information will not be provided unless the appropriate health professional has been consulted
i. Before providing the information the GP/health professional must:

    - Remove all personal information pertaining to third parties (this does not include information relating to third parties in their professional capacity, e.g. a GP)
    - Consider whether the record contains information which could be harmful to the patient. The Data Protection Act allows the health professional to deny or limit access to information in the records that would cause serious harm to the physical or mental health or condition or the patient (or any other person). Information can only be withheld from patients in limited circumstances, and the

health professional must be able to justify their reasons for doing so. There is no obligation to inform a patient that information has been withheld, particularly if it would cause the patient damage or distress to do so.

j. Before the patient is provided with the information, the identity of the person must be ascertained either by personal knowledge of the person by the clinician or by inspection (and copying) of passport or driving license or other appropriate photo-id.
k. Manual records will be photocopied and electronic records may be printed off or sent electronically if requested to do so and assurance can be provided regarding the security of doing so.[1]
l. All information must be released in a format that is intelligible to the individual. The patient should be provided with the organisation's privacy notice when providing the requested data.
m. The patient's request will be recorded in the electronic notes using code 9N5A.
n. Online access to patients' medical records may in some cases substitute for a SAR, depending on the nature and extent of the request.

*Please note, this process will also be adhered to for responding to staff member requests to data held about them.*

### 2. Fees

Under the GDPR, the organisation is not permitted to charge data subjects for providing a copy of the requested information; this must be done free of charge. That said, should a request be deemed either "unfounded, excessive or repetitive", a reasonable fee may be charged. Furthermore, a reasonable fee may be charged when requests for additional copies of the same information are made. However, this does not permit the organisation to charge for all subsequent access requests. Where requests may appear to be "unfounded, excessive or repetitive", the data controller may ask why the patient wants the information.

Any reasonable fee charged should be based on the administrative costs associated with providing the requested information.

### 3. Negotiated Disclosure

It is anticipated that with the removal of the SAR fees, that the number of requests received may increase.

As health care providers may process and hold a large quantity of information about an individual, the GDPR permits providers to ask the data subject to specify the information the request relates to. It may be possible to mutually agree to provide just the specific information that is required. For instance, just what is held on the patient's electronic record, all information from a certain date, or even details relating to a specific procedure. This must be mutually agreed between the data processor and the data subject.

- [1] Instructions for sending encrypted messages can be found here: https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/encryptionguide.pdf
- Instructions for receiving encrypted messages can be found here: https://s3-eu-west-1.amazonaws.com/comms-mat/Comms-Archive/Accessing+Encrypted+Emails+Guide.pdf
- Guidance can be found here: https://portal.nhs.net/help/policyandguidance (scroll down and click on Sharing Sensitive Information Guidance).

## 4. Declining a Request for Data

You can decline to provide a SAR, or as the GDPR states, ‘not take action’ if the request is excessive or unfounded. The DPO should be consulted before declining a request. However you’ll still have to justify why within the 28 day deadline and explain how the data subject can complain about your decision to the ICO your decision. This should be documented. One obvious reason for declining is if the data has not changed since a previous request.

Beyond the ‘excessive or unfounded’ clause you can also refuse to provide data where the patient already has the information. Other relevant exceptions include where:

- It would involve a disproportionate effort (eg, letters from the 1960s that are no longer relevant)
- It would disclose comments about a third party to the patient (except for others involved in their care)
- It could result in harm to the patient or anyone else
- The information is subject to a court order or is privileged, or subject to fertilisation or adoption legislation.

## 5. Third Party Requests Data on Behalf of a Patient

A third party, including legal representatives, can ask for patient records on behalf of a patient and you still cannot ordinarily charge for a first SAR. If you hand over data to a nominated third party for free, you have by definition provided access free to the patient because the nominated third party is the patient ‘by proxy’.

However, solicitors/insurers are not permitted to seek a SAR to support an application that should be made under the Access to Medical Reports Act (AMRA), i.e., reports for employment and insurance purposes. This covers accident claims and insured negligence as well as mortgages and life insurance – anything covered by an insurance contract that requires a medical report. If a solicitor’s letter does not make the precise purpose of the request and report clear, then ask them if the report is being requested under GDPR or AMRA. If the report is to support an actual or potential insured claim then AMRA applies. You can charge and no additional information is needed.

The same applies to employers – so if the report is in connection with proposed or actual employment, it’s not classed as a SAR, therefore you can charge and no additional information is needed.

Clause 181 of the Data Protection Bill (due to be enacted later this year) will extend the offence of ‘enforced subject access’ to cover medical records, so this will become a criminal offence. Insurers will not want to be found guilty of the crime of enforced subject access. If any GP suspects that an insurer is doing this, they should report them to the Information Commissioner’s Office and the Association of British Insurers. Guidance on this from the ABI and the BMA is unchanged under GDPR.

Where a request from a third party qualifies as a SAR, the organisation will ensure that the data subject has granted consent, as outlined above. Where it is unclear as to whether the request would be more appropriate under AMRA, the organisation will seek clarification that the request is in fact a Subject Access Request and not a request for insurance or employment purposes. The latter of which will continue to incur an administrative fee.

## 6. Access to Records of Deceased Patients

It is DoH and GMC policy that records relating to deceased people will be treated with the same level of confidentiality as those relating to living people. If a patient indicated in life that they would want their record to remain confidential, their decision must be respected.

Access to records of the deceased is governed by the Access to Health Records Act 1990. When a patient has died, their personal representative, executor, administrator or anyone having a claim resulting from the death (e.g. a relative or someone else), has the right to apply for access to the deceased patients records (i.e. the relevant part of the record relating to the claim). There are no other situations where disclosure of deceased records to a third party is permitted, except where this is to comply with some other legal obligation.

For GP records, the record holder might be the Records Department at the relevant CCG. Requests will be passed immediately to this department where it is appropriate to do so.

a. Ensure the request for access is made in writing. The request will contain sufficient information to ensure the correct records are identified, and details of the applicant's right to access the records.
b. Where appropriate, refer the request to the relevant PCT – as discussed above.
c. Ensure all health records requests are dealt with in 21 consecutive days. 40 consecutive days for all other (non-health record) requests.
d. Consider whether all information will be disclosed to the patient. A health professional can restrict access if it is felt that disclosure would cause serious harm to the physical or mental health of any other person, or would identify a third party. Such decisions MUST be justifiable.

## 7. Charging for a Request for Deceased Records:

A maximum fee of £10 can be charged, where the record has not been added to in the last 40 days preceding the application. An additional fee can be charged for copying and posting the records (see fees list). The organisation must not be seen to make a profit.

Manual records will be photocopied and electronic records may be printed off. If the patient wishes to view electronic records, care must be taken that no other information is accidently revealed.

All information must be released in a format that is intelligible to the individual.

## Appendix 4 – Procedure for Requests under the Freedom of Information Act

1. The Freedom of Information Act provides the public with a right to apply for access to information held by public bodies. It covers corporate information such as minutes of meetings, statistics, financial details
2. The act gives individuals two basic rights.

   A) To be told whether the requested information is held by a public authority.

   B) To receive the information (and where possible, in the manner requested, i.e. as a copy or summary, or the applicant may ask to inspect a record)
3. The Act covers recorded information held in any format e.g. computerised records, paper files, information in emails, recorded on post-it notes etc.
4. Requests will be dealt with by the organisation that holds the information (i.e. the originator). If requested information is held on behalf of another organisation, the request will be referred to that organisation
5. 43 exemptions exist to the provision of information. For e.g. personal information (such as patient information) is exempt from disclosure. Exemptions must only be applied by the Practice Business Manager who deals with access requests.
6. Requests must be dealt with in 20 working days (postal requests = the clock starts the day after it is received. Email requests = the clock starts on the day the email is received).
7. Requests will be passed directly to the Practice Business Manager
8. Requests must be in writing and the requester must provide a return address (either postal or email)
9. The organisation cannot charge for the request, unless the cost of providing information would exceed £450. The cost equates to 2 1/2 days of searching time, at a standard rate of £25 per hour. The cost can take account of the following activities:

- determining whether the information is held
- locating and retrieving it, and
- extracting the information (including editing)

See fees regulations at http://www.foi.gov.uk/practitioner/feesguidance.htm#part4)

Further guidance on dealing with FOL requests can be found at
http://www.foi.gov.uk/index.htm AND http://www.ico.gov.uk/

## Appendix 5 - Sharing information with other professionals

### 1. Sharing information with other health professionals

In the absence of evidence to the contrary, patients are normally considered to have given implied consent for the use of their information by health professionals for the purpose of the care they receive. Information sharing in this context is acceptable to the extent that health professionals share what is necessary and relevant for patient care on a 'need to know' basis.

Health and social care, although often closely related, do not always fall into the same category, and disclosure of information to social services usually requires explicit consent from competent patients. Sometimes two competing interests come into conflict, such as the patient's informed refusal to allow disclosure and the need to provide effective treatment to that person. A patient's refusal to allow information-sharing with other health professionals may compromise patient safety, but if this is an informed decision by a competent person it should be respected.

### 2. Multi-agency working

Health professionals during the course of their treatment of patients will have contact with partner organisations from time to time. These include social services and housing and benefits agencies. In community settings many integrated teams have been established, which include workers from health, social services and non-statutory bodies.

Health professionals should from the outset discuss with patients the desirability of sharing information with other agencies where appropriate. Other agencies may wish to be involved in discussions about patients at various points in their treatment or to attend case conferences or multi-disciplinary meetings. Health professionals may also be invited to attend external case conferences organised by partner organisations to discuss the health and welfare of patients.

In all these circumstances confidential information should be shared with explicit consent or, in the absence of consent, where disclosure is required by law or there is an overriding public interest in disclosure.

For further information, please see ‘Confidentiality: good practice in handling patient information’ (GMC.)

| | | | |
|---|---|---|---|
| **Strand Medical Group** | | | |
| **Procedure for Access Control** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

The Practice Business Manager in conjunction with the Deputy Practice Manager and the Office Administrator establishes who needs access to the computer systems within the Practice.

The Practice Business Manager decides what access level is required. The privileges accorded to each user will depend on their status within the Practice, their role and responsibilities. All access will be removed once a user leaves the Practice

The Office Administrator, as directed by the Practice Business Manager, provides the user with a unique username and password.

The user must immediately log-on and change their password. This password must not be shared or used to allow anyone else access to the computer system (see procedure for password).

The user can change or request to change their password at any time and should do so if they suspect others may know.

A user may be required to use other unique identifiers to gain access to other information systems.

A list of those who have access to the SystmOne is found on the system and that person is disabled from the system when they leave the employ of the Practice

The computer login and NHS mail login forces a password change at regular intervals.

| Strand Medical Group | | | |
|---|---|---|---|
| **Procedure for access to fax machines, servers, printers and care of printed material** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

The Practice server are located in the server room which is lockable if necessary and are only accessible to staff. SystmOne is a web based application and TPP servers are located off-site.

The main fax machine is located within the main photocopier machine in the Reception area and is only accessible to staff and GPs.

Faxes are high risk devices for accidental transfer of information to unauthorised recipients.
It is the organisation policy not to use a fax unless no other method of transmitting information is possible (email, telephone, letter). Where common recipients are used (e.g. faxing a prescription to a pharmacy) then pre-set memories will be used on the fax to reduce the risk of a wrong number.

Each consulting room has a printer for prescriptions and other documents.

Printers used for printing person-identifiable information are located in staff offices. Each staff member is responsible for timely collection of printed material containing the person-identifiable information.

Printers are sited so that passers-by cannot see confidential information being printed out, especially in case of consulting and treatment rooms.

Confidential printouts are stored securely either in locked cabinets/safe or office. These are only removed when necessary by those authorized to do so or disposed into Shred-it bins when no longer needed.

All prescription forms/pads etc. are be locked away when not in use.

Only recognised and trusted scanning software and hardware should be used e.g. scanner provided by NEL CSU; workflow processing as part of SystmOne.

| Strand Medical Group | | | |
|---|---|---|---|
| **Procedure for password choice and changing of password** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

Computer and SystmOne logon passwords are to be selected based on following rules:

- Minimum of 6 characters to be used combining letters and numbers (e.g. field2008)
- Words that are easily deduced such as surname should not be used
- Letters that are sequential either in the alphabet or on the keyboard e.g. ABCDEF or QWERTY should not be used
- The sharing of passwords is forbidden. Anyone found to be sharing password may be subject to disciplinary action.
- Passwords must not be writen down. A clue may be written and stored off-site.

Changing of password:

- Passwords for logging on to the network and to SystmOne will be changed regularly as determined by the system set up via an automatic prompt.
- The same password should not be used again for at least 12 months.
- Any password that has been breached or is suspected of being breached must be changed immediately.
- New software issued to the Practice for a trial period and issued with a built-in password will require this password to be changed immediately upon first proper use to ensure security.
- SystmOne password changes can be processed by Super Users, Office Administrators or Shift Leaders.

| **Strand Medical Group** | | | |
|---|---|---|---|
| **Procedure for log-on routines** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

**System Log-on: SystmOne**

1. The user double clicks on SystmOne icon on the shortcut menu or on the computer desktop.

2. The log-on screen appears

3. When logging in by Smartcard
   Insert Smartcard into the keyboard slot and enter passcode. Click 'Yes I accept and wish to proceed'.

4. When logging in by user name and password
   The user must type in their Login ID and password and press enter.

5. The system activates and the user is able to have access to the opening screen.

| Strand Medical Group | | | |
|---|---|---|---|
| **Procedure for maintenance, including remote maintenance** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

The Practice contacts the NEL CSU IT Services helpdesk for any assistance with regards to all computers, hardware and the printers. SystmOne has its own dedicated helpdesk.

Remote maintenance – SystmOne, NEL CSU, Opus and Crescendo have remote access to our systems. Remote Access will not be granted to anyone other than from these organizations and every effort will be taken to ensure access is by authorized personnel.

The Practice has an ongoing annual maintenance contract with their telephone supplier for the telephone system and who can access the system remotely if necessary. The Practice holds both daytime and OOH contact numbers.

Anyone entering the premises and attending to any of the above equipment is required to sign the visitors book is given a badge to identify they are permitted to perambulate around the building and also sign a Confidentiality Statement which is then kept by the Reception team.

The Practice has a renewable annual maintenance contract (current with Williams Medical) to maintain and calibrate all medical equipment.

The Practice has a renewable annual contract with Gary Mathews Builders for all general building and maintenance requirements. Maintenance log is kept by the Office Administrator who oversees any maintenance work that is done at the Practice premises.

| Strand Medical Group | | | |
|---|---|---|---|
| **Procedure for prevention of intruders** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

Reception staff are responsible for ensuring that all windows and doors are closed and locked every day before last staff member leaves the premises.

Allocated staff make sure that the burglar alarm is set for all zones and activated before last staff member leaves the premises. First staff in the morning deactivates the alarm with a fob or a passcode provided by Banham Group (Security 201). Any burglar alarm errors are to be immediately reported to either Practice Business Manager or the Office Administrator who contact the Banham Group.

Monitoring company Banham Group (Redcare) is regularly updated with a list of emergency contact numbers on annual basis. The Practice has a key holding service in place arranged with CMS Key Holding

| Strand Medical Group | | | |
|---|---|---|---|
| **Procedure for reporting of incidents and faults** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

Any member of the staff who reports any of the following is responsible for reporting any such happening:

- A stranger in the Practice
- Unauthorised person interfering with a PC
- A computer screen being observed by any unauthorised person
- Perceived fire risk
- Temporary loss of data
- Member of staff with authorised access looking at patient information not relevant to their job

The staff member involved will report this using an Incident Form or Significant Event form available to all staff in server folder \\h82011dc001\H82011-USF\~Emis-Shared-Folder\Shared\Forms\Staff and which is then passed to the Practice Business Manager.

Details of all incidents are kept in a restricted access folder on the server if electronic version or in a locked cupboard if paper version. They are discussed at Partnership, or Clinical Governance meetings with the team/s involved as appropriate.

| **Strand Medical Group** | | | |
|---|---|---|---|
| **Procedure for transferring information** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

Steps for staff to follow for individual communication means:

**Phone**

1. Establish the types of information that may be received over the telephone (check with your line manager if in doubt)
2. Always confirm the identity of the other party by asking for their name, department and organisation
3. Confirm the reason for the information request is appropriate
4. Take a contact telephone number. In order to check the identity of the other person call back on published main switchboard numbers and ask for the person
5. Before exchanging information ensure that the correct patient has been identified using at least two pieces of identifying information, such as their NHS number (preferable) or name and date of birth
6. Ensure that the information requested can be provided. If in doubt, check first and call the person back
7. Provide the information only to the person who has requested it (do not leave messages)
8. Ensure that you record your name, date and the time of disclosure, the reason for it and who authorised it. Also record the recipient's name, job title, organisation and telephone number

**Fax**

If you are faxing to a known **Safe Haven/Secure Fax**, you do not need to follow any special instructions. If not follow steps 1 to 6 below:

1. Telephone the recipient of the fax (or their representatives) to let them know you are going to send confidential information
2. Ask them to acknowledge receipt of the fax
3. Double check the fax number
4. Use pre-programmed numbers wherever possible
5. Make sure your fax cover sheet states who the information is for, and mark it "Private and 'Confidential"
6. If appropriate, request a report sheet to confirm that transmission was okay

**E-mail**

Only use email for sending sensitive personal information if encryption is available. Person identifiable information is only secure when sent from an nhs.net address to an nhs.net address. Transmission of confidential information to any other address not ending @nhs.net should have the subject prefixed [SECURE] to ensure encryption is applied.

**Post**

1. Only use reliable transport couriers
2. Protect the contents from any physical damage during transit in accordance with manufacturers specifications

3. Confirm the name, department and address of the recipient
4. Seal the information in a robust envelope
5. Mark the envelope “Private and Confidential” – “To be opened by Addressee Only”
6. The envelope can then be placed in another envelope with only the correct name and address details on it. This means that posted items are not easily identified as “Private and Confidential” and any administration staff or post room will only open the outside envelope
7. When appropriate, send the information Recorded Delivery
8. When necessary ask the recipient to confirm receipt

**Paper-based personal information**
Care should be taken to avoid using paper based personal information, even for home visits. Connect my Care laptops are available to facilitate access to electronic records remotely.

| **Strand Medical Group** | | | |
|---|---|---|---|
| **Procedure for virus protection** | | | |
| Checked by: | Deputy Practice Manager | Approved: | Yes |
| Review Date: | 24/09/2018 | Date: | 24/09/2018 |

Only software properly obtained from reputable supplies such as the NEL CSU is to be used by all members of staff.

Playing games on the Practice computers is strictly forbidden.

Virus protection software is provided by NEL CSU.

Virus scanner software is updated at regular intervals as determined by NEL CSU. In case a virus is found on the computer, it must be disconnected from the network and Office Administrator must be advised, who will contact NEL CSU helpdesk for assistance.
The virus software must on no account be switched off by anyone other than the technical support team.

Back-up of data stored on the local server is done daily by Clinical or Office Administrator; data can be retrieved based on request to NEL CSU.

All incoming memory sticks should be checked and virus scanned before using.
If the scanner finds a virus, isolate the computer and then use the scanning software to delete the virus. If this does not work contact the NEL CSU.

All incoming CDs from unverified source are to be checked on isolated computer.

Where emails are concerned, users must make sure that sender is checked before emails are opened from an unknown and suspicious source. Any such emails must be treated with caution and deleted before opening if identified as unsafe.

Any emails from members of the Practice or CWS CCG marked urgent should be opened first.

Programs must not be installed by any members of staff apart from the Practice Business Manager, Deputy Practice Manager or a member of staff member delegated directly by the Practice Business Manager.

The virus software must not be switched off by anyone other than GP technical support team.