Information Governance

Information for Patients

Information Governance (IG)

Contents:

- Identifying the IG Lead for the Practice. This identifies the main people responsible for Information Governance Policy.
- The IG Policy including Exchange of Information and Secure Transfers of Personal Data. This sets out the generic standards for managing information. It refers to many other policies in place but omitted for brevity.
- Confidentiality Policy & Individual Signature Sheet of Acceptance. This is the agreement out staff have to sign
- Email Policy. This is our email policy we expect staff to use
- Secure Transfer of Personal Information. This sets out how staff receive and send out information.
- Information Security Incident Reporting. This is what we do if things go wrong
- Training Needs Analysis for Data Security and Confidentiality. This is an example of the training needs we consider annually
- Information request form for Health Professionals. This shows the procedures and standards required when other health professionals make requests for information. This is included so that viewers can see what we do to ensure when information is shared it is done so properly.

Information Leaflets:

~ Freedom of Information Act 2000

~ 'How We Use Your Records'

~ Guidance for Staff Handling Patient Information and leaflet for visitors or Contractors.

Market Street Medical Practice

The Senior Partner, Dr J O'Donovan is the Caldicott Guardian and the Practice Manager, Louise Vine, is Information Governance Lead for the practice.

The key responsibilities are:-

- To develop an Information Governance Policy with assistance from the PCT and /or maintain the currency of the policy.
- To ensure that the practice's approach to information handling is communicated to all staff and made available to the public.
- To coordinate the activities of staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities.
- To be Caldicott Lead (Dr O'Donovan)for the practice ensuring that patient data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott principles.
- To monitor the Practice's information handling activities to ensure compliance with law and guidance.
- To ensure that training made available by the PCT is taken up by staff as necessary to support their role.

The day to day responsibilities for guidance to staff would be undertaken by the Practice Manager

Name:	Signature:	Role:	Date:
Dr J O'Donovan		Caldicott Guardian	31.12.08
Louise Vine		Information Governance Lead	31.12.08

Market Street Medical Practice

INFORMATION GOVERNANCE POLICY

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 and structures provide a robust governance framework for information management.

2. Principles

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Practice 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 Practice 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 Practice believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of everyone in the Practice to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

2.1. Openness

- Non-confidential information about the Practice and its services should be available to the public through a variety of media, in line with the Practice's code of openness
- The Practice maintains policies to ensure compliance with the Freedom of Information Act
- The Practice undertakes annual assessments and audits of its policies and arrangements for openness
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- The Practice have clear procedures and arrangements for liaison with the press and broadcasting media
- The Practice have clear procedures and arrangements for handling queries from patients and the public

2.2. Legal Compliance

- The Practice regards all person identifiable information, including that relating to patients as confidential
- The Practice will undertake or commission annual assessments and audits of its compliance with legal requirements
- The Practice regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- The Practice maintains policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality
- The Practice maintains policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

2.3. Information Security

- The Practice maintains policies for the effective and secure management of its information assets and resources
- The Practice will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Practice will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Practice maintains incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security

2.4. Information Quality Assurance

- The Practice maintains policies and procedures for information quality assurance and the effective management of records
- The Practice commissions annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- The practice promotes information quality and effective records management through policies, procedures/user manuals and training

3. Responsibilities

It is the role of the Senior Partner in the Practice to define the Practice's policy in respect of Information Governance, taking into account legal and NHS requirements. The Senior Partner is also responsible for ensuring that sufficient resources are available to support the requirements of the policy.

The designated Information Governance Lead in the Practice is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the Practice, raising awareness of Information Governance and ensuring that there is ongoing compliance with the policy and its supporting standards and guidelines.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they remain aware of the requirements incumbent upon them for ensuring compliance on a day to day basis.

4. Policy Approval

The Practice acknowledges that information is a valuable asset, therefore, it is wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, protecting the interests of all of its stakeholders.

This policy, and its supporting standards and work instruction, are fully endorsed by the PCT through the production of these documents and their formal approval by the Practice.

We will, therefore, ensure that all staff, contractors and other relevant parties observe this policy in order to ensure compliance with Information Governance and contribute to the achievement of the [insert organisation type] objectives and delivery of effective healthcare to the local population.

Senior Partner _____

Date _____

Market Street Medical Practice

CONFIDENTIALITY POLICY

In the course of your employment or associated work with the Practice, you may have access to, see or hear, confidential information concerning the medical or personal affairs of patients, staff or associated healthcare professionals. Unless acting on the instructions of an authorised officer within the practice, on no account should such information be divulged or discussed except in the performance of your normal duties. Breach of confidence, including the improper passing of registered computer data, will result in disciplinary action, which may lead to your dismissal.

You should also be aware that regardless of any action taken by the Practice, a breach of confidence could result in a civil action against you for damages.

You must ensure that all records, including VDU screens and computer printouts of registered data, are never left in such a manner that unauthorised persons can obtain access to them. VDU screens must always be cleared when left unattended and you must ensure you log out of computer systems, removing your password. All computer passwords must be kept confidential.

No unauthorised use of the internet or email is allowed.

Information concerning patients or staff is strictly confidential and must not be disclosed to unauthorised persons.

This obligation shall continue in perpetuity.

Disclosures of confidential information or disclosures of any data of a personal nature can result in prosecution for an offence under the Data Protection Act 1998 or an action for civil damages under the same Act in addition to any disciplinary action taken by Practice.

I have read, understand and agree to the terms and conditions set out above.

Signature……

Name (printed)……

Date……

Market Street Medical Practice

Exchange of Information

Introduction

This standard is in place to prevent loss, modification or misuse of information exchanges between organisations. Information is sometimes exchanged with other health professionals to enable the care of a person to be progressed efficiently and safely. We operate a strict policy for ensuring this exchange is done properly and appropriately. The protocol and arrangements for this are available to view on the website under Information Requests by Health Professionals and at the end of this document.

Risk Management

The risks identified under this policy include unauthorised access to information, misuse of information, loss of information, unauthorised disclosure of information, breach of legislation.

1.0 Information Exchange Agreements

1.1 Agreements are established for the exchange of information and software (whether electronic or manual) between organisations and they consider:

- management responsibilities for controlling and notifying transmission, despatch and receipt
- procedures for notifying sender, transmission, despatch and receipt
- minimum technical standards for packaging and transmission
- courier identification standards
- responsibilities and liabilities in the event of loss of data
- use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected
- information and software ownership and responsibilities for data protection, software copyright compliance etc
- technical standards for recording and reading information and software
- any special controls that may be required to protect sensitive items, such as cryptographic keys.

2.0 Security of Media in Transit

2.1 The following controls are applied to safeguard computer media being transported between sites.

- reliable transport or couriers will be used. A list of authorised couriers will be agreed and procedures to check the identification of couriers will be implemented
- adequate packaging will be used to protect the contents from any physical damage likely to arise during transit and will be in accordance with manufacturers' specifications.
- additional controls will be applied where necessary to protect sensitive information from unauthorised disclosure or modification, for example:
    - use of locked containers
    - delivery by hand
    - tamper-evident packaging
    - use of digital signatures and encryption

3.0 Security of Electronic Office Systems

3.1 Guidelines have been developed and implemented to control the business and security risks associated with electronic office systems.

4.0 Publicly Available Systems

4.1 A formal process has been implemented to ensure that information is authorised before being made publicly available and the integrity of such information will be protected to prevent unauthorised modification.

5.0 Other Forms of Information Exchange (e.g. faxes, mobile phones)

5.1 Procedures are in place to protect the exchange of information through the use of voice, facsimile and video communications facilities and should include:

- Staff know that they should take appropriate precautions, e.g. not to reveal confidential / sensitive information such as to avoid being overheard or intercepted when making a phone call
- Staff know that they should not have confidential conversations in public places or open offices and meeting places with thin walls.
- Not leaving messages on answering machines in line with the general policies on confidentiality
- Not writing confidential / sensitive information on white boards

5.2 Guidelines and protocols have developed and implemented for the use of facsimile.

Policy adopted 31.12.08

Market Street Medical Practice

Email Policy

All individuals who are authorised to use e-mail facilities are required to comply with this policy.

Individual Responsibilities:

All employees, contractors, sub-contractors and temporary staff are responsible for their personal use of email facilities provided to or used by the Practice.

The Practice Manager is responsible for providing and maintaining a standard e-mail disclaimer and for setting and monitoring acceptable usage and mailbox rules.

The Practice Manager is responsible for identifying appropriate training materials to ensure that users of the e-mail service are aware of the provided email functionality and their responsibilities for good working practices.

The PCT shall respond to and manage reported information security incidents, and shall ensure adequate corporate anti-virus protection and cryptographic controls exist in line with published NHS Good Practice Guidelines

Expected and Acceptable Uses:

Email may not be used for communicating illegal material, defamatory content, personal harassment, non-business purchases, or for publishing unauthorised views or opinions that may be damaging to the Practice. Use of the Email service may be monitored for compliance with this policy.

All emails shall have an inserted footer that contains a legal disclaimer. Users of the service may not alter or delete this.

The Practice's e-mail service may only be used for the communication of NHS information in accordance with NHS Information Governance Codes of Practice.

The communication of NHS Confidential or NHS Restricted information by email must be appropriately protected, using approved cryptographic controls (currently AES 256 bit strength or equivalent). When using NHSmail this technical security protection is automatic.

Email users must avoid opening incoming e-mail attachments that have not been checked for possible viruses or other malware in case they cause damage or disruption to the service.

Good Practice:

Spam, Viruses, Chain mail and Phishing messages:

Email users must remain vigilant to the potential threats posed by email and are required to report any suspicious messages they may receive to the Practice Manager immediately, for possible isolation and investigation.
It is prohibited to send any such messages onto other email users.

Email users are expected to apply good working practices to avoid where possible:

- the use of group e-mailing functions;
- copying of email to unnecessary recipients;
- the use of the "reply to all" function;
- the use of the blind copying feature.

Email users are expected to comply with published Incident Reporting Procedures for the Email service concerned and as may be periodically revised.

Email users are required to maintain their email boxes in good working order ie to delete e-mail messages when no longer required. Off-line email archive facilities should only be used in accordance with the Practice's published guidelines and must take account of records management obligations including Data Protection and Freedom of Information.

Email users may not use the email service for personal transactions that may be confused or perceived as official business.

Emails may only be forwarded in the user's absence to another email service where (a) that email service has been approved in advance for this purpose by the PCT and the Practice and (b) the other email service provides an equivalent level of information security protection.

Breaches of this email policy may potentially result in local disciplinary action and or criminal prosecution for the service user concerned.

I have read, understand and agree to the terms and conditions set out above.

Signature:……Date:……..

Name (printed)……

Policy adopted 31.12.08

Market Street Medical Practice

Secure transfers of personal data: safe havens

Introduction:

Everyday the Health Service collects vast amounts of information, this could be about you, your family, friends, neighbours or people that you know, but the majority of this information will belong to total strangers that you are unlikely to ever meet. This information is not the property of the Health Service. It belongs to the people that it has been collected from.

The Health Service is merely the custodian, as custodians we are responsible for the safe keeping and security of all information that comes into our keeping.

As a data collector and information user you are responsible for ensuring that you handle this information with care and respect. It is your responsibility to protect this information from those who are not authorised to use it or view it. You must ensure that whilst in your care you have done everything possible to protect this information, and comply with the Caldicott Principles and Data Protection requirements.

These guidelines will hopefully increase your awareness of some of the problems you may encounter when sending transferring/transmitting personal information and help you ensure that you have done all that you can to keep the information you wish to transmit as secure as possible.

Definitions:

- **Safe Haven:**

The term **safe haven** is term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles.

- **Personal information:**

Personal information is information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

- **Sensitive Personal Information:**

Sensitive personal information is a category of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community, for example, where the personal information contains details of the individual's:

- Health of physical condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Trade union
- Political opinions
- Criminal convictions

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

Requirements for Safe Havens /Location/ Security Arrangements

Confidential information is received to a specific location in the Practice:

- The room/area is sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to visitors.
- The room/area is on the ground floor with appropriate measures for physical security, and protected by 24 hour monitored intruder alarm systems.
- The room/area conforms to health and safety requirements in terms of fire, flood, theft or environmental damage.
- Manual paper records containing personal information are stored in locked cabinets when not in use and in a separately locked room when the building is not in use.
- Computers should not be left on view or accessible to unauthorised staff and should have a secure screen saver function and be switched off when not in use.

Communication by post:

- Written communications containing personal information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. Where appropriate, they should be clearly marked "Personal and Confidential – to be opened by the addressee only".
- The designated person should be informed that the information has been sent and should make arrangements within their own organisation to ensure that the envelope is delivered to them unopened and that it is received within the expected timescale.
- All mail is to be opened at a central point. An alternative means of transfer can be arranged where it is essential that the information is restricted to those who have a need to know.
- The personal information contained in written transfers should be limited to those details necessary in order for the recipient to carry out their role.

Communication by email:

- Transfer of personal information by email should be avoided unless the information is encrypted i.e. transmitted in a coded format. NHSmail is the only British Medical Association and Department of Health approved email service for securely exchanging clinical data between NHSmail users. Therefore email should not be used for sending confidential information unless both sender and recipient are using an NHSmail account.

- Otherwise
  - a risk assessment should be undertaken by Caldicott/IG Lead in conjunction with the partners.
  - the attachment should be encrypted.

Verbal communication:

- A considerable amount of information sharing takes place verbally, often on an informal basis. Difficulties can arise because of this informality particularly in modern open plan offices. Care should be taken to ensure that confidentiality is maintained in such discussions.
- If information is to be shared by phone, then steps need to be taken to ensure the recipient is properly identified. This can be done by taking the relevant phone number, double checking that it is the correct number for that individual / organisation and then calling the recipient back.
- Where information is transferred by phone, or face to face, care should be taken to ensure that personal details are not overheard. Where possible, such discussions should take place in private locations and not in public areas, common staff areas, lifts etc.
- Messages containing personal information should not be left on answer machines.
- Messages containing confidential / sensitive information should not be written on white boards / notice boards where they can be seen by anyone other than practice staff.

Communication by fax:

One of the most common breaches of confidentiality occurs when documents that contain patient identifiable information are sent by fax machine. Many fax machines are in corridors or open plan offices and are used by several different departments. People come and go collecting faxes but do not always check that all the pages belong to them; this increases the risk of information being seen by unauthorised persons.

To combat this, many NHS organisations have designated certain fax machines as 'Safe Haven' machines. These are machines that are located in a secure area and are used to receive documents of a private and confidential nature. The Practice has policies and procedures in place for the handling of confidential information received by fax, e.g. ensuring an appropriate person is responsible for collecting and delivering any faxed information to the appropriate person.

If you are sending a fax to another organisation, ask if they have a Safe Haven fax machine.

No Safe Haven Fax machine?

If the organisation that you need to fax does not have a Safe Haven fax machine, then follow a few simple rules

DO …

- Telephone the recipient of the fax let them know that you are about to send a fax containing confidential information
- Ask if they will wait by the fax machine whilst you send the document
- Ask if they will acknowledge the receipt of the fax
- Make sure that you have clearly stated on the fax cover sheet that the information you are sending is confidential. Please see below for a suggested form of words*.
- Check the fax number you have dialled and check again that it is correct before sending
- Request a report sheet to confirm that the transmission was O.K.
- If this fax machine is going to be used regularly, store the number in your fax machines memory.

The information contained in this fax is **STRICTLY CONFIDENTIAL** and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately. Thank You

DO NOT…

- Send faxes to where you know that the information will not be seen for a time.
- Send faxes at times that maybe outside the recipients hours of work
- Leave information unattended whilst a fax is being transmitted

If you receive confidential information on your fax machine, it is your responsibility to inform the sender that you have received this information.

This guidance covers personal information about staff as well as patients

TREAT ALL PERSONAL INFORMATION AS IF IT WAS ABOUT YOU.
THINK HOW YOU WOULD LIKE IT TREATED.

This policy adopted 31.12.08

Market Street Medical Practice

Information Security Incident Reporting

Introduction

Information security is everyone's responsibility; this policy has been developed to ensure Market Street Medical Practice employees identify information security incidents, suspected information security weaknesses or near misses or security threats to services or systems and report these incidents through appropriate management channels for investigation and follow up.

An Information Security Incident

An information security incident is any violation of the Practice's Information Governance (IG) /Information Security Policy. The term information security incident and suspected incidents is very broad and includes, but is not limited to, incidents that relate to the loss, disclosure, denial of access to, destruction or modification of the Practice's information, or information systems.

An information security incident can be defined as any event that has resulted or could result in:

- The disclosure of confidential information to an unauthorised individual
- The integrity of a system or data being put at risk
- The availability of the system or information being put at risk

An adverse impact can be defined for example as:

- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of Practice business
- An embarrassment to the Practice

Examples of security incidents:

- Using another user's login id/swipe card
- Unauthorised disclosure of information
- Leaving confidential / sensitive files out
- Theft or loss of IT equipment

- Theft or loss of computer media, i.e. floppy disc or memory stick
- Accessing a persons record inappropriately e.g. viewing your own health record or family members, neighbours, friends etc.,
- Writing passwords down and not locking them away
- Identifying that a fax has been sent to the wrong recipient
- Sending/receiving an sensitive email to/from "all staff" by mistake
- Giving out or overhearing personally identifiable information over the telephone
- Positioning of pc screens where information could be viewed by the public
- Software malfunction
- Inadequate disposal of confidential material

Diligent employees should question procedures, protocols and events that they consider could cause damage, harm, distress, break of compliance or bring the Practice's name into disrepute.

Reporting of Security Incidents

All information security incidents should be reported to [the Practice Manager, who will ascertain the level of risk and ensure any immediate action is taken appropriate to the level of risk. All incidents will need to be formally recorded on an incident report form and, if appropriate logged to the Practice's risk management or incident reporting system (e.g. PRISM). The responsible officer in the Practice will investigate, document and if necessary provide feedback on the outcome of the incident.

All significant incidents relating to information security should be reported to the PCT's Information Governance Lead and Caldicott Guardian, particularly in instances where these involve bulk data loss or confidentiality breaches.

A log will be kept of all incidents reported, irrespective of whether they lead to a complaint or not. All incidents should be considered as to whether they indicate a need for improvement in arrangements. The log may be incorporated into other incidents logs as appropriate. A regular report on the number, type and location of information security incidents should be made, allowing any trends to be picked up and addressed.

By reporting such incidents or near misses it allows the Practice to relate to similar occurrences and highlights any areas of vulnerability, identifying where greater awareness is needed, or procedures/ protocols that require reviewing. Good reporting generates better statistical data thus, keeping the Practice informed.

When reporting an information security incident, it is important to ensure sufficient information is given to the IG lead to enable them to understand and respond appropriately to the report. Users can report security related incidents in confidence; no information about a user's involvement in a security incident will be released without explicit permission.

If reporting software malfunctions, symptoms of the problem and any messages appearing on the screen should be noted. The PC should be isolated and the use of it stopped, until reported. Users must not attempt to remove suspected software or attempt to 'repair/mend' equipment unless authorised to do so.

Description of Incident

It is important that the information security incident reports give as much detail as possible. Including a description of activities leading up to the security incident, information about circumstances prevailing at the time, how the incident came about, how the incident was detected.

The information security incident or suspected incident report should include full details of the incident in as much details as possible to enable a full investigation to be carried out if necessary. However, when logging incidents, personal details should, wherever possible, be omitted.

Whenever possible when reporting information security incidents, any protocols or procedures which may have been compromised should be referenced on the report.

All information security incidents will be prioritorised in accordance with the severity of the incident by the person logging these on the risk or incident reporting system.

The [*insert name of practice*] policy requires that information security incidents be reported as soon as possible after they occur, or have been identified. Reports sent immediately after the incident are likely to be the most valuable; if there is a delay between an incident occurring and the discovery of said incident, the incident should still be reported.

Follow Up

Incidents should be used in training sessions about security and confidentiality as using 'real life events' relevant to a practice can always be related to by staff, a lot better than in imaginary events. This will give the attendees and example of what could occur, how to respond to such event and how to avoid them in the future.

This policy adopted 31.12.08

Training

All employees need to have annual refresher training on all aspects of Data Security and Confidentiality. The following document is designed to act as a guide when training is being planned.

Employee Name _____

Job Title _____

Have you received appropriate training on the following topics, within the last year?

	Yes	No	Unsure
Physical Security of Manual Records			
Physical Security of Computer Records			
Computer Passwords			
Access to Patient Data			
Confidentiality and the Use of Patient Identifiable Information			
Media Handling (Storage/Transfer/Disposal)			
Telephone Enquiries			
Safe Haven Procedures			
Legal Requirements			
Caldicott Guidelines			
Sharing Information with Other Organisations			
Security of the Building			

Are there any other areas of data security and confidentially that you feel you need further training on?
……
……
……

Signature of Employee _____ Date _____

Name of Manager _____

Action / Training plan:
……

Signature of Manager _____ Date _____

Market St Medical Practice
Form for requesting details from a GP record.

This form must be completed by a suitably trained health or social care professional who is registered with a regulatory authority. The form **must** be signed.

Person for whom information is requested:

Name, DoB, NHS No, Address We will not provide information if the demographics are mismatched or insufficient to identify the subject of the request.

Requesting Team/Authority/Person:

Please provide a full response. The name of the hospital alone is insufficient.

Reason for Request:

Please provide as full a response as possible. Generic requests like "hospital policy" will be rejected as we cannot justify the release of confidential information without good reason.

If this is a **clinical** emergency you must say why.

Amount of information required:

Dates/Content etc. Please avoid requesting the complete record. It may run to a hundred pages and take a long time to compile. This will delay the release of information. Lengthy records will not be faxed.

Place to which the information should be sent and person to whom it should be addressed.

AGREEMENT

In requesting this information the requester acknowledges their responsibility to comply with confidentiality procedures and law on data protection. The requester also must accept the disclaimer. Providing this information is costly and time consuming for the NHS. Multiple requests from the same organisation or for the same purpose from different organisations will be rejected. If anything untoward or inaccurate is discovered in the record you must inform us.

DISCLAIMER

This information in the record is **confidential** and is only released for the purpose for which it was requested. It must not be shared with anyone who is not authorised or used for any other purpose.

This is a GP record and **not** a complete record of health or illness. It is compiled in part from information provided to us by many other people some of whom may not be health professionals. Consequently, whilst every reasonable effort is made to ensure the accuracy of the record we cannot guarantee it against errors or omissions.

As our records may be updated on a daily basis, this record may be out of date the day after you receive it. Information that has not been sent to us in a timely fashion may be missing. Information may be inserted into the record retrospectively as we record events on the date they occurred not the date we received the information.

Information on laboratory tests are not included as they are available to view online via the INDIGO 4 system. You must contact your system administrator if you cannot access that system.

The prescription history may only include medicines we prescribe. There are many other healthcare professionals who may also be prescribing for this person.

This record should not be used as a substitute for proper clinical practice.

In accepting this information you must agree to the above conditions without exception.

SIGNED……

POSITION……

DATE……

For office use

Sent on……by……