**DR S V SHARMA’ SURGERY**

**BILSTON HEALTH CENTRE  
PROUDS LANE  
BILSTON   
WEST MIDLANDS  
WV14 6PW**

**CONFIDENTIALITY POLICY**

This policy identifies patient expectations for confidentiality and specifies how the Practice will undertake to protect those expectations. In addition this policy highlights how the Practice will comply with the laws on Data Protection, Human Rights, Common Law Duty of Confidentiality etc.

The Policy complies with the Code of Practice for Confidentiality as published by the NHS, and includes sample posters and leaflets for the purposes of making staff and public aware of confidentiality issues. These need further refining and discussion.

Author: - Phil Turner

Version: - 1.0

Date: - November 2007

Reviewed: - November 2010

Next Review: - November 2012

Status: - Live

# 1. Contents

1. Contents
2. Policy Statement
3. Purpose
4. Background
5. Patient’s Expectations
6. Principles of Confidentiality
7. Meeting the requirements for confidentiality
8. Guideleines for the Protection of Confidentiality
9. Conclusion

Appendix I Information Governance Monitoring of Caldicott

Appendix II Legislation surrounding Confidentiality

Appendix III Confidentiality Posters and Leaflets for Patients (for further discussion)

Appendix IV Confidentiality Code of Conduct for Staff (for further Discussion)

Appendix V NHS Models for the Disclosure of Personal Information

# 

# Policy Statement

# In the course of your duties you may have access to confidential material about patients, members of staff or other health service business. On no account must information relating to identifiable patients be divulged to anyone other than an authorised person, for example medical, nursing or other professional staff, as appropriate, who are concerned directly with the care, diagnosis and / or treatment of the patient. If you are in any doubt whatsoever as to the authority of a person or body asking for information of this nature you must seek advice from your superior officer. Similarly, no information of a personal or confidential nature concerning individual members of staff should be divulged to anyone without the proper authority having first been given. However it is recognised that information sharing is an integral part of delivering care and that failure to share may cause more harm than good. Failure to observe these rules will be regarded by your employers as serious misconduct and which could result in serious disciplinary action being taken against you, including dismissal.

# Purpose

The purpose of this policy is to:

* Establish a Practice-wide approach to ensuring the confidentiality of person identifiable information.
* Inform members of the public, patients and carers about the Practice’s confidentiality obligations and how it intends to meet them.
* Inform staff working for, or on behalf of, the Practice of their responsibilities with regards to confidentiality and person identifiable information and how the Practice will enable these to be met.

This policy links to the Practice’s policies covering Data Protection, Records Management and IM&T Security. Together these policies form an integral part of the Practice’s approach to Information Governance.

# Background

**4.1 Policy context**

Respect for confidentiality is an essential requirement for the preservation of public confidence in the Practice.

The Caldicott Committee, which reported in 1997, was established to review the confidentiality and security requirements across the NHS with regard to person identifiable information. The Committee recommended a series of six principles that should be applied when considering whether such confidential information should be shared.

These principles, details of which are provided in Section 6.2, were developed with the aim of establishing the highest practical standards for handling confidential information. The principles apply equally to all person identifiable information whether clinical or non-clinical, manual, computerised, visual, audio recorded or held in a member of staff’s head.

All NHS organisations and Social Services Departments are now required to apply these principles and to nominate a senior person to act as a **Caldicott Guardian** responsible for safeguarding the confidentiality of person identifiable information.

Caldicott Guardians have a strategic role in developing security and confidentiality policies, representing confidentiality requirements at Board level, advising on annual improvement plans and agreeing and presenting annual outcome reports. The Guardian, and staff working on their behalf, maintains an ongoing advisory role to deal with issues concerning the confidentiality of person identifiable information.

Other Caldicott recommendations listed in HSC 1999/012 identified actions that should be undertaken by Trusts in support of the Guardian, namely to:

* Develop local protocols governing disclosure of patient information to other organisations.
* Restrict access to confidential information within each organisation by enforcing strict ‘need to know’ principles.
* Regularly review and justify the uses of confidential information.
* Improve organisational performance across a range of related areas: database design, staff induction, training, and compliance with the Caldicott Guidance.

Appendix I gives details of the Management Audit Organisation Profile against which the Practice has annually to report its progress. This has recently been updated in light of the publication of the Information Governance Toolkit.

Following public consultation in 2002 the Department of Health has developed a nation-wide confidentiality code of Practice for all NHS staff. The content of this policy takes into account the content of that Code of Practice.

**4.2 Local Context**

The Practice provides services to a population of some 3100, residents of Wolverhampton, as well as referrals from surrounding Health Areas. There are 2 Partners and 10 staff working in the Practice. In addition, the Practice is accredited for the training of medical students and Advanced Nurse Practitioners.

In providing these services the Practice works closely with Wolverhampton City Primary Care Trust, The Royal Wolverhampton Hospital Trust, Keele University Medical school and the University of Wolverhampton. In addition the Practice has links with Wolverhampton Metropolitan Borough Council and other independent practitioners such as dentists, opticians and pharmacists. To differing extents across the borough, the Practice staff share a mixture of facilities, electronic and manual record management systems and access to patients information with these agencies.

Irrespective of where, how, with or to whom else Practice provides its services the requirements for confidentiality remain of the same high standard and applies to all individuals who have worked or are working for, or on behalf of, the Practice.

4.3 Legislative context

The guidance contained in the Caldicott Committee report is only one of a number of legal and statutory requirements, and other guidance, related to maintaining the confidentiality, security and protection of person identifiable and anonymised information with which the Practice must comply.

Key additional legislation and guidance includes:

* Access to Health Records 1990
* Data Protection Act 1998
* Crime and Disorder Act 1998
* Human Rights Act 1998
* Freedom of Information Act 2000
* Health and Safety at Work
* Child Protection
* Crime and Disorder act 1998.

The Practice and all staff who work for, or on its behalf are subject to a Common Law Duty of Confidentiality. This duty of confidence only applies to person identifiable information and not to aggregated or anonymised data.

All Practice staff are subject to a confidentiality clause in their contracts of employment. Breaches of confidentiality by staff may therefore lead to disciplinary action being taken against them.

In addition all health professionals have professional and ethical duties of confidentiality within their codes of conduct.

Appendix II provides further details of the above-mentioned legislation and guidance.

# Patient’s Expectations

The patient / client has a right to be secure in the knowledge that all information given to a health care professional is given in confidence in the expectation:

* That it will be used only for the purposes outlined in the patient publications and will not be released to others without their consent.
* That it will be held in private and secure storage
* That, where it is deemed appropriate to share information obtained in the course of professional Practice with other health or social work practitioners, or in the case of children, education services, the health care professional who obtained the information must ensure, as far as is reasonable, before its release that it is being imparted in strict professional confidence and for a specific purpose.
* That where it is deemed appropriate to share information obtained in the course of professional Practice with other health and social work practitioners, or in the case of children, education services, the patient client is aware of this, the reasons for it and where there may be disclosure of information to others not directly involved in the client's / patient's care given the opportunity to withhold consent.
* That the responsibility to either disclose or withhold confidential information lies with the individual practitioner
* That he / she cannot delegate the decision.
* That he/she cannot be required by a superior to disclose or withhold information against his / her will
* That a health care professional who chooses to breach the basic principle of confidentiality in the belief that it is necessary in the public interest including that of protecting a child must have considered the matter sufficiently to justify that decision
* That deliberate breaches of confidentiality other than with the consent of the patient / client should be exceptional
* That when a health care professional is considering disclosure of confidential information, Practice has a duty to ensure that the individual staff member can seek and gain appropriate advice through their line manager, their professional body and Caldicott Guardian who may wish to consult the Trust's legal advisors
* That when, after due consideration and seeking appropriate advice, the health care professional decides it is necessary to breach confidentiality without consent of the patient / client and can justify that decision, that person does so acting as an employee of Practice and therefore will be supported by the Trust in their action.

# Principles of Confidentiality

**6.1 General Principle**

“Confidentiality” can be generally defined as ‘when personal information is given or received in confidence for a particular purpose. This information may not then be used for a different purpose or passed on to anyone else without the consent of the information provider.’

However, there may be occasions when it could be detrimental to the patient or to another individual if this principle was strictly adhered to.

An example of such an exception would be child protection where the overriding principle is to secure the best interests of the child. Anyone holding information that is relevant to the protection of a child/children **must** share that information with others on a strictly controlled basis. Several major child abuse inquiries have identified the lack of such communication as being a contributing factor in the death of a child.

### *Most breaches of confidence are unintentional. They are often caused by staff conversations being overheard, by files being left unattended, or by poor computer security, however the consequences could be equally serious for all concerned. The simple rule of thumb is that person identifiable information should always be held securely and, when used, treated with respect. This rule applies whether the information is held manually or in a computer, on video or audio tape or in a member of staff’s head.*

**6.2 Caldicott Principles**

The following six Caldicott principles should be adhered to in all cases where the appropriate use of person identifiable health information is considered.

**Principle 1 Justify the purpose(s) -** every proposed use or transfer of person identifiable information within, or from, an organisation, should be clearly defined and scrutinized. The Caldicott Guardian should regularly review continuing uses.

**Principle 2 Don’t use person identifiable information unless it is absolutely necessary -** person identifiable information should not be used unless there is no alternative.

**Principle 3 Use the minimum necessary person identifiable information -** where person identifiable information is considered to be essential, the use of each individual item of information should be justifiable, the aim being to reduce the risk of an individual being identified.

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

**Principle 5 Everyone should be aware of their responsibilities -** action should be taken to ensure that those recording, storing, handling and using person identifiable information (both clinical and non-clinical staff) are aware of their responsibilities and obligations in respect of respect confidentiality.

**Principle 6 Understand and comply with the law -** every use of person identifiable information must be lawful. A nominated person within each organisation should be responsible for ensuring that the organisation complies with legal requirements and with the requirements for Caldicott.

Examples of justifiable purposes include:

* Delivering personal care and treatment.
* Assuring and improving the quality of care and treatment.
* Monitoring and protecting public health.
* Managing and planning services.
* Contracting for the NHS.
* Auditing NHS accounts and accounting for NHS performance.
* Risk management.
* Investigating complaints and notified or potential legal claims.
* Teaching.
* Statistical analysis.
* Medical or health services research.

Appendix III provides guidelines for staff on key factors relating to confidentiality.

These guidelines do not and cannot provide definitive answers for every situation as much depends on the context of the individual case. If in doubt staff should seek appropriate advice before releasing person identifiable information.

# Meeting the requirements for confidentiality

People have a right to expect that information about them, provided or discovered in the course of their health care, will be held in confidence. Without assurances about confidentiality, people may be reluctant to provide information and this could lead to unnecessary restrictions on what most people rightly perceive as the essential purpose of providing it: the delivery of appropriate and effective care to themselves.

To meet confidentiality requirements of patients, carers and staff the Practice has, or has in development, the following policies, procedures and/or processes in place.

* Confidentiality and Data protection staff training and induction programme
* Code of Conduct for handling personal identifiable information
* Data Protection Act Policy
* Access to Health Records procedures
* Access to Employee Records procedures
* Clinical and non clinical records management policy
* IM&T Security policy
* Inter-Agency Information Sharing Framework and protocols
* Safe Haven guidance
* Guidance for the safe transmission of faxes
* Confidentiality Pledge Poster - Informing the public (Appendix IV)
* Contract of employment - Confidentiality clause
* Breach of confidentiality and Data Protection notification procedures
* Annual Management Audit report

All staff throughout the Practice have a responsibility for maintaining confidentiality and should be aware of how the content of the above-mentioned policies, procedure and processes affects their actions on a day-to-day basis.

Appendix IV provides more information about the different levels of responsibility for confidentiality throughout the Practice.

# GUIDELINES FOR THE PROTECTION OF CONFIDENTIALITY

### Most breaches of confidence are unintentional. They are often caused by staff conversations being overheard, by files being left unattended, or by poor computer security, however the consequences could be equally serious for all concerned. The simple rule of thumb is that person identifiable information should always be held securely and, when used, treated with respect. This rule applies whether the information is held manually or in a computer, on video or audio tape or in a member of staff’s head.

If in doubt – check it out - before releasing person identifiable information

### 8.1. Obtaining Consent

As a general rule personal information given for one purpose may not be disclosed to a third party or used for another purpose without the consent of the person it relates to, unless the third party is at risk.

Within the Health Service it may not be practical to obtain the consent of the patient every time information needs to be shared with other professionals involved in the care of that patient. Therefore it is necessary for the Practice to remind patients of their rights regarding confidentiality and inform them in what circumstances and for what purposes their personal information may be shared.

All new patients should be provided with the Practice’s leaflet which explains why personal information about them may need to be shared with other professions and agencies. Similarly, at a patient’s first appointment, clinicians should take the opportunity to discuss and explain the need for the sharing of personal information. Specific consent to the sharing of person identifiable information must always be sought for situations not covered by the Practice’s leaflet and in particular when information has to be shared with services outside the Practice.

In this latter case, the patient should be advised that if consent is withheld, there could be implications for the quality of care that can be offered. The clinician should, with the patient, investigate the reasons for withholding consent and attempt to arrive at a satisfactory solution where the care given would be least compromised.

**8.2. Informing Relatives**

Whilst the routine provision of information about a patient’s condition to a near relative or a person with a close relationship to the patient, should not be obstructed unnecessarily, the provision of information should be at the discretion of the service and should reflect any wishes of the patient.

If before death a patient gives requests that the relatives or carers do not see their medical records, then this must be recorded in the Medical Notes and the wish respected after death.

Under Caldicott the clinician has the ultimate decision regarding the sharing of the medical notes with other parties, providing it is done with the express purpose of helping the patient. It is a responsibility which cannot be delegated. Advice can be sought from other clinicians (typically the Caldicott Guardian) or from the relatives and carers, but ultimately the decision lies with them.

The Relatives or Carers have no over-riding power to give consent on behalf of the Patient.

If the patient is under 16 information may be passed to their guardian unless they expressly oppose this or unless the professional involved felt that this would put the child at risk.

If the child has a life threatening condition the parents or guardian should be approached regardless. Guidelines on confidentiality with regard to children can be found at section 4 of this appendix.

**8.3. Withholding Information**

### If a patient requests that a specific piece of personal information be withheld from someone then this view should be respected, unless there are overriding considerations. The reason the patient gives for not passing on the information must be noted. An overriding consideration may include the statutory obligation that staff have to work together with other agencies as stated in the Children’s Act 1989 and the Mental Health Act 2004.

**8.4. Consent of Children**

Children under the age of 16 or 17, who in the view of the health care professional have the capacity and understanding to take decisions about their own treatment, are entitled to decide whether personal information may be passed on. This may be particularly relevant if a child does not wish his/her parent to know, however the child should be encouraged to involve parents or other legal guardians.

If the child has a life threatening condition the parents or guardian should be approached regardless

**8.5. Inability to Give Consent**

If for any reason a patient was incapable of giving consent for their information to be shared, the professionals concerned (who may or may not be part of a multi disciplinary team) would make the decision, taking into account the best interest of the patient. This will include considering the views of relatives, carers or advocates, and any views the patient may have had, if at some stage he/she had the capacity to decide.

However the clinician cannot delegate that responsibility to share or not share that information. Providing adequate consultation has taken place with line managers and the Caldicott Guardian, then the Practice is obliged to support that clinician’s decision, even if they choose go against the advice given.

**8.6. Retention and Disposal of Information**

The retention and disposal of personal information in either a manual or computer format is addressed in the "Records Management Strategy and Policy" and the "Disposal of Media Policy". Information from which a person can be identified must always be disposed of securely.

**8.7. Disposing of Electronic Data**

Guidance on the disposal of electronically stored data that includes personal information will be obtained from the PCT’s Information Governance Manager.

**8.8. Recording of information**

Decisions regarding the use of personal information should be clearly recorded within individual patient’s records and authorised by the member of staff responsible for making the decision.

**8.9. Confining Information**

Within the Practice a large number of staff, both professional and administrative will see personal information. It is therefore vital that the principle of confidentiality is maintained. This would include all personal information about members of the public, not just their medical records. Names should not be exchanged unless there is a need to do so.

**8.10. Sharing Information**

The six Caldicott Principles should be adhered to in all cases where the sharing of person identifiable information is being considered. In addition, if information is being shared outside the NHS, a formal Information Sharing Protocol should be implemented.

In addition the three models of Disclosure as described in the NHS Document “Confidentiality:- Code of Practice” must be followed. (Appendix VI)

### 8.11. Occasions for Disclosure

Disclosure of confidential information should only occur if the individual gives consent *or* on a "need to know" basis if the reasons are deemed justifiable. Section 7 of the Health and Safety at Work Act states that if a risk is identified to someone else’s health and safety and that person is not informed of the risk, the individual identifying the risk is in breach of the Act. This may include information regarding a patient or carer, which may put others at risk.

### 8.12. Seeking Advice

In the event that the Health Care Professional responsible for the patient's care is required to pass on information, they are responsible for passing the *minimum* information necessary for the purpose. If needed they should take advice from a senior professional or manager who may themselves seek advice from the Caldicott Guardian.

**8.13. Breaking Confidentiality**

If a health care professional chooses to break confidentiality because it is deemed to be in the best interest of the public, i.e. due to the violent history of a patient, the decision must be carefully considered as it may need to be justified. In such a case, the health care professional should consult with the Practice Manager, who may then seek advice from the Caldicott Guardian. Such decisions should be clearly recorded in the patient’s records.

**8.14. Protecting the Public**

There may be instances when staff working for, or on behalf of the Practice feel obliged to pass on information to protect the public or for the purpose of averting a serious crime. This type of disclosure should be made in consultation with the Caldicott Guardian, unless specifically allowed within one of the Practice policies. The Practices’s Communications, Serious Untoward Incident and Whistle blowing policies provide further guidance on this issue. When decisions of this type are taken, a permanent record of the decision should be made and held in an appropriate place. Each case should be considered individually, but it may be necessary to seek advice from a manager. On occasions, legal advice may be necessary. There is no absolute definition of "serious crime", but section 116 of the Police and Criminal Evidence Act 1984 identifies some "serious arrestable offences". These include:

Treason,

* Murder and manslaughter,
* Rape and certain sexual offences
* Kidnapping and the taking of hostages,
* Causing an explosion and offences under the prevention of terrorism legislation,
* Certain firearm offences,
* Hijacking,
* Causing death by reckless driving,
* Making a threat which if carried out would be likely to lead to:
* a serious threat to the security of the state or to public order
* serious interference with the administration of justice or with the investigation of an offence

- death or serious injury

- substantial financial gain or serious financial loss to any person

### 8.15. Information to the Media

As a general rule no information is to be given to the media in respect of current or previous patients, carers or staff. The passing of personal information to the press or media is covered by the same general principle, that is, if the person whom the information is about is capable of taking a decision their consent must be obtained. Likewise if the individual is incapable of making the decision, information should only be given if it is in the best interests of the person concerned. The Caldicott Guardian should decide who is the most appropriate member of staff to speak to the media. The Practices’s Communications, Serious Untoward Incident and Whistle blowing policies provide further guidance on this issue.

### 8.16. Multi-agency Protocols

Where at all possible multi-agency protocols should be developed to cover the transfer of information. A generic protocol exists which can be used as a framework throughout the borough. The Information Governance Manager can give advice.

### 8.17. Ensuring Confidentiality

* Clear Desk/ clear screen policy
* VDU Positioning so no-one else can see the screen
* Ensuring conversations are not overheard
* Ensuring information is received by the right people
* Fax Machines located in Safe Havens (Safe Haven Policy)
* Secure emails (Safe haven and eMail Policy)

### 8.18 Processing Information Requests

When information is requested from anyone other than the Subject or a clinical function, the provision of identifiable information should be avoided the possible methods are as follows

* **Anonymisation**  
  Information should be non-identifiable. Under data protection even a code number (ie NHS Number ) which can be related back to an individual, no matter how closely guarded that code is makes the information identifiable. Small samples with postcodes will similarly make identification possible.
* **Aggregated Data**

Again small sizes of samples could lead to identification. Provided patients are aware that aggregated and statistical info will be prepared it is all right to continue.

### 8.19 Teaching and Research

Advice to patients about the use of personal information must emphasise:

* the importance of teaching and research to the maintenance and improvement of care within the NHS
* that such information, anonymised or aggregated wherever possible, may sometimes be used for teaching and research (and that universities or other bodies carrying out approved research are required to treat it in confidence and must not use it for other purposes).
* that any research proposals involving access to patient records require clearance by the relevant Local Research Ethics Committee. (LREC approval is not required for epidemiological surveys conducted for the purpose of communicable diseases surveillance and control).

The Local Research Ethics Committee must be satisfied in particular that:

i. arrangements for confidentiality are satisfactory   
  
ii. any additional conditions relating to the use of information that the LREC thinks are necessary can be met   
  
iii. any application to use identifiable patient information is fully justified e.g. because this is essential to a study of major importance to public health. If not, approval would not be given.

* that their specific consent will be sought to any activity relating to teaching or research that would involve them personally

that published research findings will not identify them without their specific agreement

### 8.20. Restrictions on passing on information

NHS bodies or those carrying out NHS functions must not allow personal details of to be passed on or sold for fund-raising or commercial marketing purposes.

There are some statutory restrictions on the disclosure of information relating to HIV and AIDs and other sexually transmitted diseases, assisted conception and abortion.

# Conclusion

## *The public, patients, carers and staff have a right to expect that all information about them will be treated as confidential, but must also recognize that there are times when the Practice may be required to share this information.*

Practice recognises the need to ensure that appropriate policies, procedures and processes are in place to maintain the highest practicable standards for handling confidential information balanced with the need to provide effective services and support.

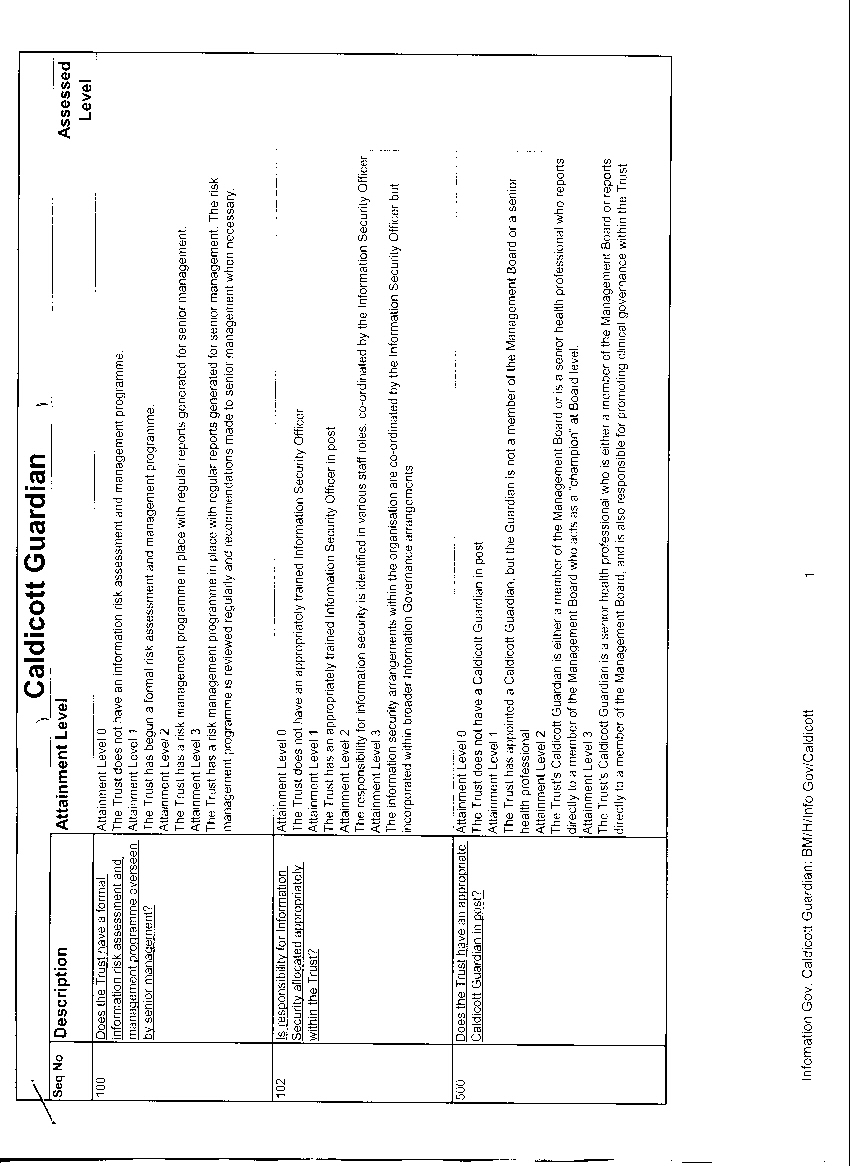
Practice is committed to:

* Endorsing and supporting the role and work of the Caldicott Guardian and associated support staff.
* Informing the public, patient, carers and staff of action taken to maintain the confidentiality of their personal information.
* Providing training, guidance, information, advice and support for all staff working for, or on behalf of, the Practice with regards to their responsibilities in relation to confidentiality and patients, carers and other members of staff.
* Having systems in place to identify where and how the Practice can improve its performance on confidentiality and associated Information Governance requirements.

## 

**APPENDIX I**

**Information Governance Monitoring of Caldicott and Confidentiality (example)**



**APPENDIX II**

**Legislation surrounding Confidentiality**

**Access to Health Records Act 1990**

This Act provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased’s estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements. The Data Protection Act 1998 supersedes the Access to Health Records Act 1990 apart from the sections dealing with access to information about the deceased.

**Data Protection Act 1998**

The key legislation governing the protection and use of identifiable patient/client information (Personal Data) is the Data Protection Act 1998. The Act does not apply to information relating to the deceased.

This Act gives seven rights to individuals in respect of their own personal data held by others. They are:

* Right of subject access
* Right to prevent processing likely to cause damage or distress
* Right to prevent processing for the purposes of direct marketing
* Rights in relation to automated decision making
* Right to take action for compensation if the individual suffers damage
* Right to take action to rectify, block, erase or destroy inaccurate data
* Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

In addition, the Act stipulates that anyone processing personal data comply with eight principles of good Practice. These principles are legally enforceable.

**Principle 1** – Personal data shall be processed fairly and lawfully

**Principle 2** – Personal data shall be obtained only for one or more specified lawful purposes

**Principle 3** – Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.

**Principle 4** – Personal data shall be accurate and, where necessary, kept up to date.

**Principle 5** – Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that or those purposes.

**Principle 6** – Personal data shall be processed in accordance with the rights of data subjects under this Act, including the right to access their own record.

**Principle 7** – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss.

**Principle 8** – Data shall not be transferred outside of the European Economic Area

Detailed information for staff about the requirements of the Act in relation to information sharing are available in the **“Data Protection Act Policy”**.

**Crime and Disorder Act 1998**

The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power but only where it is necessary and expedient for the purposes of the Act. However, whilst all agencies have the power to disclose, Section 115 does not impose a requirement on them to exchange information and responsibility for the disclosure remains with the agency that holds the data. It should be noted, however, that this does not exempt the provider from the requirements of the 2nd Data Protection principle.

The Criminal Procedures and Investigations Act 1996 requires the police to record in durable form any information that is relevant to an investigation. The information must be disclosed to the Crown Prosecution Service, who must in turn disclose it to the defence at the relevant time if it might undermine the prosecution case. In cases where the information is deemed to be of a sensitive nature then the CPS can apply to a judge or magistrate for a ruling as to whether it should be disclosed.

**Human Rights Act 1998**

Article 8.1 of the Human Rights Act 1998 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. This is however, a qualified right i.e., there are specified grounds upon which it may be legitimate for authorities to infringe or limit those rights and Article 8.2 provides “there shall be no interference by a public authority with the exercise of this right as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedom of others”.

In the event of a claim arising from the Act that an organisation has acted in a way which is incompatible with the Convention rights, a key factor will be whether the organisation can show in relation to its decision to take a particular course of action:-

* That it has taken these rights into account
* That it considered whether any breach may result, directly or indirectly, from the action, or lack of action
* If there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights
* Whether one of the permitted grounds for interference could be relied upon
* Whether there was proportionality

The Act also requires public bodies to read and give effect to other legislation in a way which is compatible with these rights and makes it unlawful to act incompatibly with them. As a result these rights still need to be considered, even when there are special statutory powers to share information.

**Common law duty of Confidentiality**

All staff working in both the statutory and independent sector are aware that they are subject to a common law Duty of Confidentiality and must abide by this. The duty of confidence only applies to identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e., it is not possible for anyone to link the information to a specified individual.

The Duty of Confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g., to protect others from harm). Whilst it is not entirely clear under law whether or not a common law Duty of Confidence extends to the deceased, the Department of Health and professional bodies responsible for setting ethical standards for health professionals accept that this is the case.

Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained (deceased individuals may have provided their consent prior to death). Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence.

Where it is judged that an individual is unable to provide consent (for example due to mental incapacity or unconsciousness) other conditions in schedule 2 and 3 of the Data Protection Act 1998 must be satisfied (processing will normally need to be in the vital interest of the individual).

Whilst under current law, no-one can provide consent on behalf of an adult in order to satisfy the common law requirement, it is generally accepted that decisions about treatment and the disclosure of information should be made by those responsible for providing care and that they should be in the best interests of the individual concerned.

All agencies are subject to their own codes or standards relating to confidentiality.

**Freedom of Information Act 2000**

This Act provides clear statutory rights for those requesting information together with a strong enforcement regime. Under the terms of the Act, any member of the public will be able to apply for access to information held by bodies across the public sector. The release of personal information remains protected by the Data protection Act 1998.

**Other legislation – summary details not provided**

Criminal Procedures and Investigations Act 1996

Regulation of Investigatory Powers Act 2000

Health and Social Care Act 2001 (Section 60)

Children Act 2004

Criminal Justice Act 2003

**There are statutory restrictions on passing on information linked to:**

NHS (Venereal Disease) Regulations 1974

Human Fertilisation and Embryology Act 1990

Abortion Regulations 1991

**Third Party Disclosures**

This applies when information is shared between organisations/agencies for a defined purpose then passed onto either another agency without consent or used for a different purpose without securing the consent from the original provider.

Controls surrounding this should be made clear in the specific Information Sharing Protocol addressing how information should be shared between the agreed parties.

**APPENDIX III**

**CONFIDENTIALITY POSTER AND LEAFLET FOR PATIENT INFORMATION**

PracticeARE COMMITTED TO ENSURING CONFIDENTIALITY OF ALL INFORMATION RECORDED ABOUT YOU AND YOUR CARE

***“Providing you with the best care possible means we need to keep up to date and accurate National Health Service records. Our pledge of confidentiality means that only appropriate members of staff who are directly clinically involved in your care are allowed access to the personal information on your record. Stringent ethical and professional standards are rigidly adhered to so that you can be sure of absolute discretion and confidentiality at all times.”***

**We have a duty to:**

Ensure we have accurate and up to date information to assess your health care and treatment.

Look after the health of the general public.

Manage and plan the NHS – for example:

- make sure that our services can meet patient needs in the future

* audit accounts
* prepare statistics on NHS performance and activity (where steps are taken to be sure you can not be identified)
* investigate complaints or legal claims

Help staff to review the care they provide to make sure it is of the highest standard

Train and educate staff (but you can choose whether or not to be involved personally)

Carry out research approved by the Local Research Ethics Committee. (If anything to do with the research would involve you personally, you will be contacted to see if you are willing to take part. You will not be identified in any published results without your agreement.)

You have a right of access to your health records.

If you agree your relatives, friends and carers will be kept up to date with the progress of your treatment.

All staff working within the NHS have a legal duty to maintain the highest level of confidentiality about patient information.

Your medical records are used to help the NHS provide you with the best possible care.

*If at any time you would like to know more about how we use your information you can speak to the person in charge of your care or ask them to provide details of how to contact the Information Governance Manager for the Practice.*

**Appendix IV**

**Confidentiality Code of Conduct for Staff**

**Practice**

**STAFF CODE OF Practice:- CONFIDENTIALITY**

**Caldicott Principles for handling patient-identifiable information.**

**Justify the purpose**.

Every proposed use or transfer of patient-identifiable information within or from another organisation should be clearly defined. (and reviewed if continuing)

**Identifiable information used only if it is absolutely necessary**.

Patient-identifiable information items should not be used unless there is no alternative

**Only 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 identification

**Access to patient-identifiable information should be restricted 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 they need to see

**All should be aware of their responsibilities**.

Action should be taken to ensure that all staff are aware of their responsibilities and obligation to respect patient confidentiality

**Comply with and understand the law.**

Every use of patient-identifiable information must be lawful.

**General Principles**

**Safeguard confidential information by following the basic rules listed below.**

**Take care to whom you disclose personal information (patient or personnel type information)** Do not disclose personal information to anyone who is not authorised to receive it - This includes hospital and other NHS and social care staff not directly involved in the care of the patient/person

**Keep your Computer Password Secure and don’t share it with anyone else. -** If you suspect someone knows your password then you should immediately change it , seeking help if necessary. Contact your manager and advise them of a potential breach of security and then complete an “Untoward Incident Form” and submit it to the Risk Management Department. Do not write down your password.

**Do not use someone else's password to gain access to information-** All systems have the facility to 'audit' who accesses them, at what time and on what date. If you don’t have a password for a system, then you are not authorised to use that system. It will be a breach of discipline if you continue to try to access that system. If for work purposes you need that access, then arrange to be trained on the relevant system and get your own password.

**Log out of your computer if leaving it unattended for any time.** – You are accountable for any actions taken on the computer while you are logged in, even if someone else has used your password.

**Do not leave patient's health records unattended,** especially in public areas.

**Do not download patient identifiable information from the hospital systems, or any other personal information for that matter, onto another computer system** unless you are authorised to do so, by the Caldicott Guardian and Head of Health Informatics

**All information must be, to the best of your knowledge, accurate and up-to-date.** If you are unsure of whether data is accurate, check with the person providing the information. All staff have a legal responsibility to ensure that the information they supply is accurate. (Data Protection Act 1998)

**Do not access information about yourself, your relatives or friends** - You do not have an automatic right to such information. You should request access to your information via the 'subject access' route.

**If requested to provide personal information over the phone, or by fax, check the identity of the caller carefully.** There should be an agreed procedure for doing this. Check the fax number is correct, send a single sheet fax initially, and check that it has been received at the other end (and vice versa). If you must send confidential information via a fax, ensure someone is there to receive it and be sure that it will not 'sit' on the fax machine for more than five minutes. Confidential information should not be given over the telephone - how do you know the person is who they say they are, particularly if it is an unknown person and do you have clear authorisation to release the information. Follow the **“Safe Haven Policy”**

**Do not put confidential waste into the normal waste bin**. Consider shredding the documentation. If shredding on-site is not an option, how do you ensure that the information is stored securely until such time as it is disposed of? Do you know your organisations policy?

**Seal all confidential correspondence or notes which are being sent through the internal or external mail system.** Make sure the envelope is address is correct, clearly written and marked confidential, for addressee only. Consider the use of recorded delivery, this allows an audit if the records do go astray. What is that organisations policy for protecting the information?

**Be sure that conversations concerning patients are not overheard.** Don't use patient names when speaking about patients in public areas or on the telephone.

*As laid down in the Terms and Conditions of Employment any breach of confidentiality may lead to disciplinary action being taken*

**Finally, Do Not Hesitate To Seek Advice When You Need It**

**People who can help you:**

Your Manager

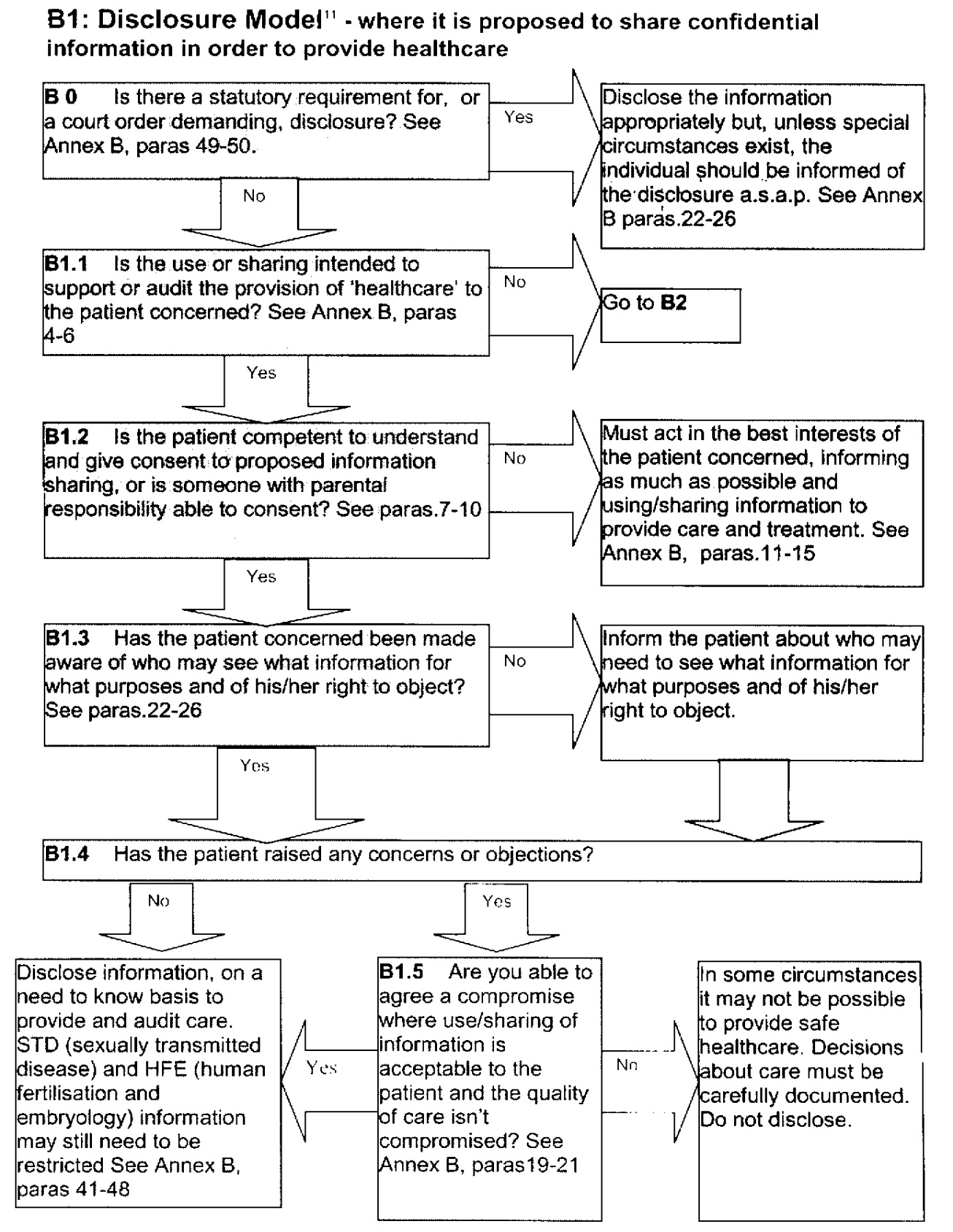
The Caldicott Guardian- PHIL TURNER (Practice Manager)

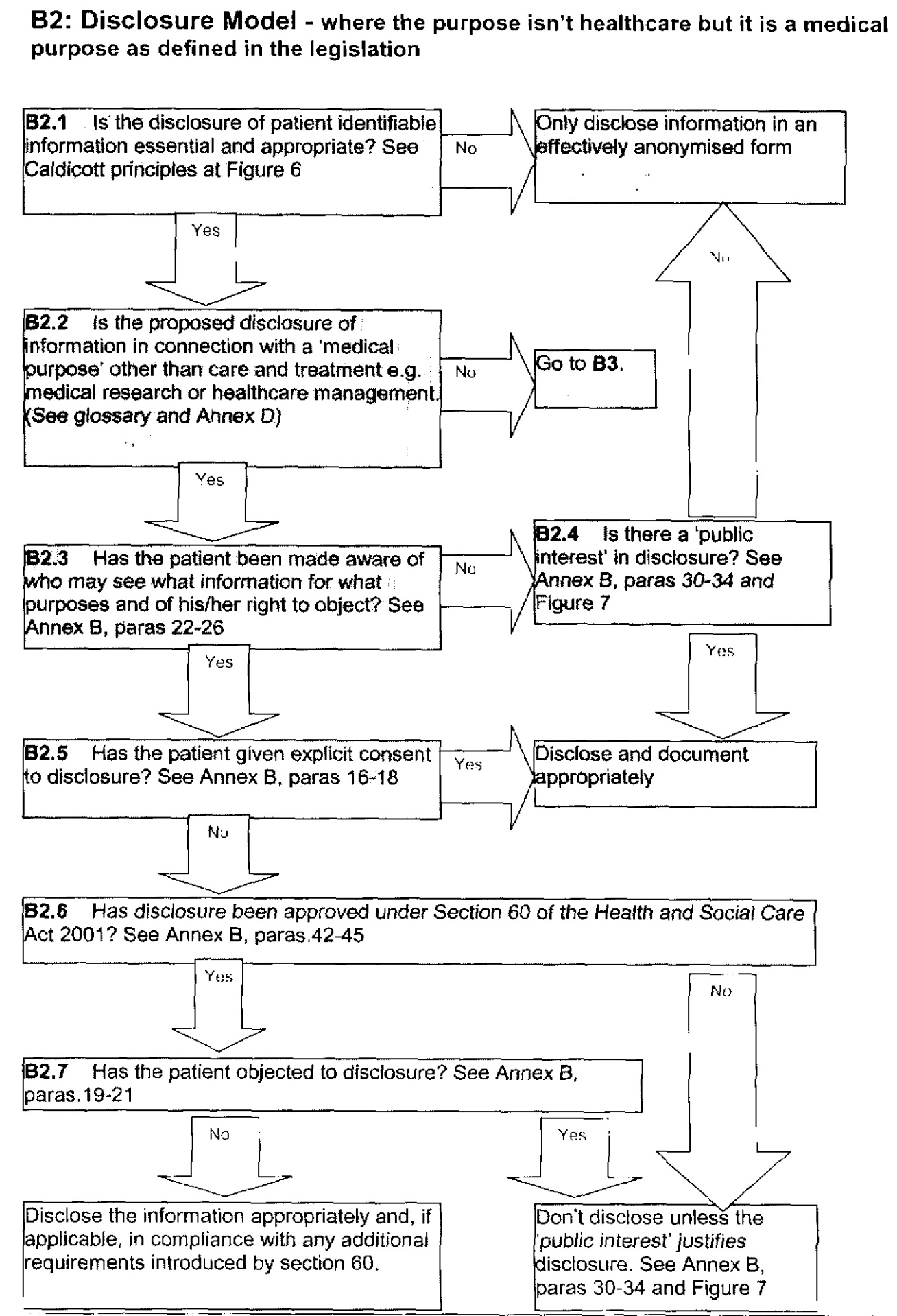
Information Governance Lead- PHIL TURNER (Practice Manager)

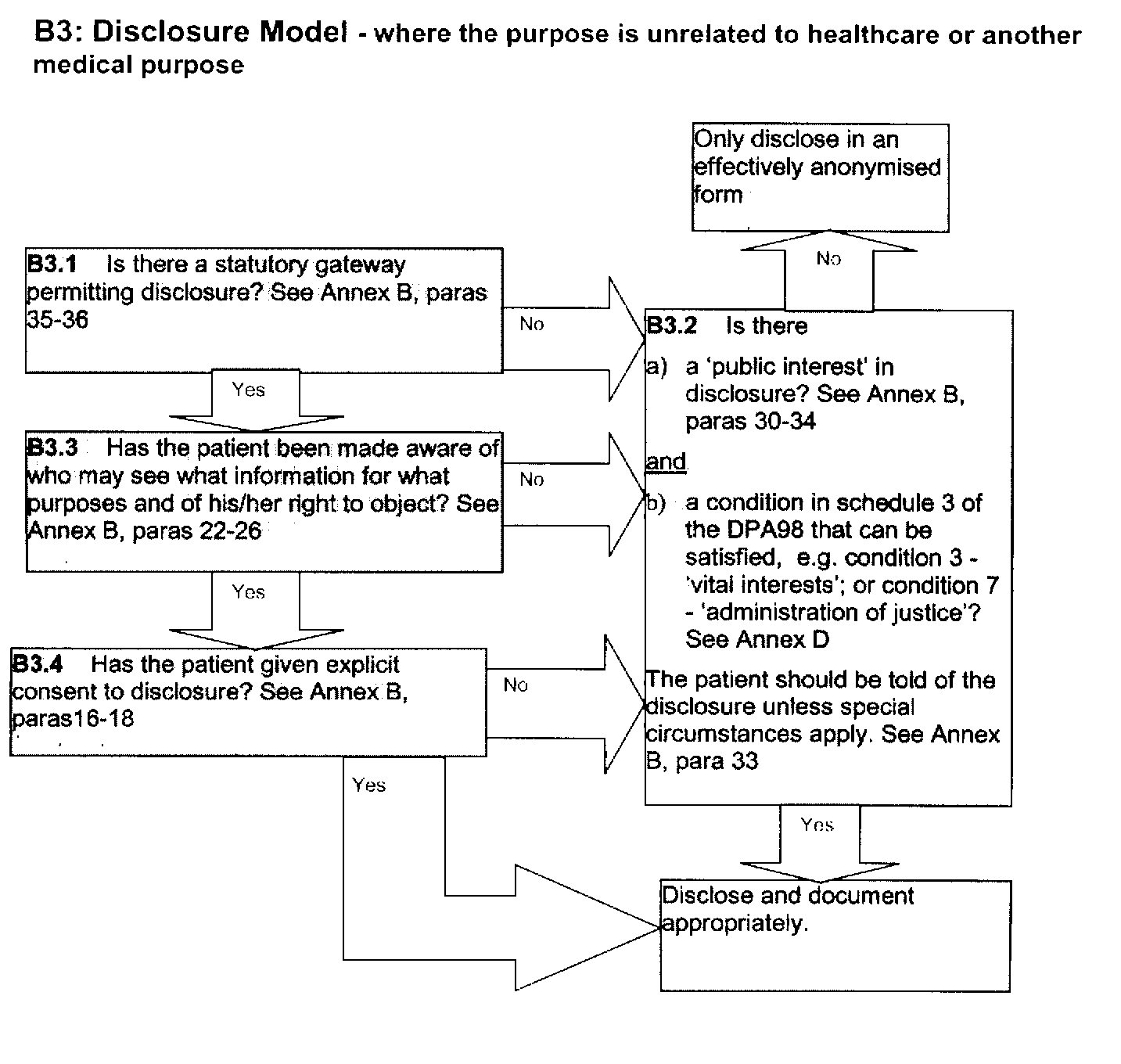
WCPCT Information Governance Advisor JENNIFER FERNANDEZ

**Appendix V**

**NHS Models for the Disclosure of Personal Information**

****

****

****