Pennine Care NHS
NHS Foundation Trust

Policy Document Control Page

Title

Title: Information Sharing Policy

Version: 6

Reference Number: CO13

Supersedes
Supersedes: Version 5
Description of Amendment(s):

Important Notice
From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator

Originated By: Jenny Spiers

Designation: Information Governance Manager

Equality Impact Assessment (EIA) Process

Equality Relevance Assessment Undertaken by: Information Risk Manager
ERA undertaken on: 17 May 2012
ERA approved by EIA Work group on: 1 June 2012

Reviewed as appropriate: Kevin Tarleton, Information Risk Manager; 11 March 2015

Where policy deemed relevant to equality-
EIA undertaken by Information Risk Manager
EIA undertaken on 1st June 2012
EIA approved by EIA work group on 1st June 2012

Approval and Ratification

Referred for approval by: Information Governance Manager

Date of Referral: 1st March 2017

Approved by: Information Governance Assurance Group

Approval Date: 1st March 2017

Date ratified by Executive Directors: 20th March 2017

Executive Director Lead: Medical Director

Circulation

Issue Date: 23rd March 2017

Circulated by: Information Department

Issued to: An e-copy of this policy is sent to all wards and departments

To be updated to the Trust's external website? Yes

Review

Review Date: February 2019

Responsibility of: Jenny Spiers

Designation: Information Governance Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 23rd March 2017

Contents

1. INTRODUCTION

1.1 Government policy places a strong emphasis on the need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services.

1.2 The Government has also emphasised the importance of security and confidentiality in relation to personal information and has strengthened the legislation and guidance in this area in particular through the Data Protection Act 1998 and the Information Governance Assurance Programme.

1.3 In May 2011, the Information Commissioner issued a data sharing code of practice specifying that "under the right circumstances, and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service …. but…. rights under the Data Protection Act must be respected. Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness."

1.4 Much of the information that needs to be shared involves personal details about service users and their needs. Current practice on the ground in relation to information sharing may vary considerably. Some staff may be reluctant to share any personal information about service users because of uncertainties about current legislation and guidance. This can lead to serious difficulties in ensuring that services are properly co-ordinated. Other staff may be unaware of the implications of recent changes and may be continuing to share information on the basis of informal arrangements. These arrangements may not comply with guidance or the law and this can leave individuals and the Trust at risk of possible legal action.

1.5 The aim of this policy is to:

- Establish a mechanism for the exchange of information between the Trust and other health, social care and public and voluntary sector organisations.
- Advise staff of the legal position with regards to sharing health information so that they are able to share appropriate information with the right people at the right time.

1.6 The Information Governance Toolkit requirement [1]207 specifies "When confidential personal information that can identify an individual is shared, both the disclosing and receiving organisations should have

[1] The Information Governance Toolkit is a performance tool produced by the Health and Social Care Information Centre (HSCIC). It draws together the legal rules and central guidance relating to information governance and presents them in one place as a set of information governance requirements. Organisations are required to carry out self-assessments of their compliance against the IG requirements.

procedures that meet the requirements of law and guidance and make clear to staff the appropriate working practices. In some circumstances these procedures (and the law and guidance on which they are based) should be set out within an agreed information sharing agreement or protocol." (See also 4.2.)

1.7 The Caldicott report recommended that organisations should draw up and implement information sharing protocols in order "to protect patients confidentiality as well as facilitate the transfer of information freely between partner organisations on a need to know basis for justifiable purposes".

1.8 The Caldicott 2 report *Information: to share or not to share* introduced a new Caldicott principle (7), that the duty to share personal confidential data can be as important as the duty to respect service user confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

1.9 Although not a legal requirement, by agreeing information sharing protocols with partner organisations the Trust will have assurance that the partner organisation is committed to the same standards of confidentiality and security as the Trust (see section 4).

1.10 The Information Sharing Policy is an official policy of the Trust. Compliance with Trust policies is a condition of employment and breach of a policy may result in disciplinary action. In addition, breaches of confidentiality and information security can result in criminal or civil action against individual members of staff.

2. SCOPE

2.1 This policy applies to all personal confidential data (PCD)[2] held by the Trust, or information held by its employees, and covers information held in computer systems, in manual records or as electronic images.

2.2 It does not include disclosure of health records that fall under the Access to Health Records policy.

3. INFORMATION SHARING PROTOCOL

3.1 Through the Greater Manchester Information Governance group, the Trust has agreed the format of an information sharing protocol to be signed up to with partner organisations (Appendix A). The protocol

[2] Previously referred to as Person Identifiable Data (PID)

promotes good practice, staff training and organisational responsibilities around confidentiality.

3.2 Attached to the protocol is a mechanism for listing information flows that have been agreed and justified by the Trust's and partner organisation's Caldicott Guardian or Information Governance/Data Protection Lead.

3.3 A template for listing these information flows is attached at Appendix B, with a completed example at Appendix C.

3.4 For ease of use, rather than listing all data items contained within the flow of information, a list of definitions has been developed and is attached at Appendix D.

3.5 The Trust has signed the protocol with a number of partner organisations. A list of organisations signed is available on the Trust Internet site.

3.6 A set of Frequently Asked Questions (FAQs) and a checklist for staff is attached which gives guidance on sharing personal confidential data (PCD) (Appendix E).

3.7 There may be circumstances in which a more detailed protocol may need to be agreed for specific areas. These will set out detailed purposes and operational procedures for the sharing of information. These can be developed in liaison with the Information Governance Manager who can provide some template examples.

3.8 The existence of a protocol between the Trust and its partners is to promote best practice. In the event of a protocol not being agreed this does not mean that appropriate information will not be shared and existing legislation and guidance will be followed both where a protocol is signed and where it is not.

4. INFORMATION SECURITY ARRANGEMENTS IN PARTNER ORGANISATIONS

4.1 The Trust reserves the right not to sanction the exchange of any information unless it is satisfied with the security and confidentiality policies and associated arrangements within the third party organisation.

All third party organisations must:

- Operate within the principles established by the Data Protection Act 1998 and, where appropriate, the additional recommendations of the Caldicott Report.

- On request, provide the names of the organisation's Information Governance Manager(s), Data Protection Manager(s) and/or responsible manager who will be the contact within the organisation for information sharing (these details will be held by the Information Governance Manager).

4.2 Information Governance Toolkit

Requirement 207 specifies that "organisations that are achieving an adequate level of performance (i.e. attainment level 2 or above) against the NHS Operating Framework key IGT requirements can be regarded as 'trusted organisations' for information sharing purposes where the purpose of sharing is the delivery of care. These organisations will all be working to the same standards and will be taking appropriate action to satisfy legal requirements and hold information securely. Senior personnel in these organisations, e.g. NHS Chief Executives, Directors of Adult Social Services, sign an IG Assurance Statement (formerly an IG Statement of Compliance) to provide the required assurance to partner organisations.

4.3 Therefore, organisations are not required to put in place information sharing protocols where information sharing is between 'trusted organisations' for care purposes. Such protocols may still be of value however where organisations feel that it is important to establish working procedures, contact points etc. that support day to day operational activity.

4.4 Where organisations are unable to demonstrate the required information governance performance to be classified as 'trusted', routine information sharing continues to require information sharing protocols in order to ensure that the 'rules' are clearly understood and that the requirements of law and guidance are being met. This is not to say that these organisations are failing to deliver effective information governance, rather that there is no agreed means for them to demonstrate that they are doing so in the absence of an agreed protocol, e.g. they are not mandated to complete the IG Toolkit.

5. SHARING INFORMATION

5.1 In all circumstances of information sharing, staff will follow the legislation and national policy i.e. the Data Protection Act 1998, the common law duty of confidentiality, and Caldicott principles for personal or patient identifiable data and only release such information under one of the following circumstances: -

a) With the informed consent of the individual (see section 6);
b) For medical purposes (including preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services), which is undertaken by: -

- A health professional (as defined in the Data Protection Act 1998 (see Appendix F), or
- A person who owes a duty of confidentiality, which is equivalent to that which would arise if that person were a health professional.

c) When the information is required by statute or court order;
d) Where there is a serious risk to public health;
e) Where there is risk of serious harm to self or other individuals;
f) For the prevention, detection or prosecution of serious crime[3];
g) The needs of the children as paramount under the Children Act, 2004 and authoritative guidance for professionals;
h) Knowledge or belief of abuse or neglect[4];
i) Circumstances detailed in any Dangerous Offenders protocol;
j) To protect the vital interest of the subject[5];
k) For the purpose of obtaining legal advice, and establishing, exercising or defending legal rights;
l) By order of the Secretary of State;
m) For the purpose of safeguarding national security.

5.2 If it is not clear at the time, advice on when any of the above conditions may apply in relation to the sharing of information can be obtained from the Information Governance Manager 0161 716 3899.

5.3 **Flowcharts for sharing patient information**

The NHS Confidentiality Code of Practice[6] documents three models for the disclosure of confidential patient information as follows:

Model B1	disclosures to support or audit healthcare[7]
Model B2	disclosures for other medical purposes (see 5.1b)
Model B3	disclosure for non-medical purposes

The models are enclosed at Appendix H.

---

[3] NHS Code of practice: Confidentiality specifies - The definition of serious crime is not entirely clear. Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality. Serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant breach of confidence.

[4] The Confidentiality policy specifies: If the health professional believes the service user to have been a victim of neglect or abuse, s/he should disclose relevant information to the appropriate person or agency, provided such disclosure is in the service user's best interests. The health professional should inform the service user of his/her intention before any such disclosure takes place. If the health professional decides that disclosure is not in the best interests of a neglected or abused service user, the health professional must be prepared to justify his/her decision.

[5] This condition may only be claimed where the information sharing is necessary for matters of life and death

[6] The full NHS Code of Confidentiality is available on the Trust intranet in the Governance section under Information Governance or from the Information Governance department.

[7] These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.

6. CONSENT

6.1 Informed consent

The service user must be told precisely what information is being requested, by whom and why before their fully informed consent can be obtained. The service user's case-notes and/or a consent form should be used to detail the key elements of the discussion with the patient, including the nature of the information provided to the third party.

6.2 Where a service user lacks capacity

Where a service user is assessed as not having the capacity to give informed consent to disclosure, the decision to disclose personal information should be governed by what is considered to be in the service user's 'best interests'. Consideration also needs to be given to whether there is a Lasting Power of Attorney that needs to be consulted. Decisions to disclose information in the service user's best interests should be taken by the health professional, and may involve discussion amongst the whole health care team. Whenever possible, the clinician with overall responsibility for care must be consulted. Additionally, in some circumstances, the views of the service user's relatives or carers may be appropriate in helping to make a decision regarding disclosure.

6.3 Children and young people

As stated in the Trust's Confidentiality Policy young people aged 16 or 17 are regarded as adults for purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults. Children under 16 who have the capacity and understanding to make decisions about their own treatment are entitled also to decide whether personal information may be passed on and generally to have their confidence respected (e.g. they may be receiving treatment or counselling about which they do not wish their parents to know[8]). In other instances, decisions to pass on personal information may be taken by a person with parental responsibility in consultation with the health professionals involved.

7. SHARING INFORMATION AT THE REQUEST OF THE SERVICE USER

7.1 Information can be transferred to another service at the request of a service user unless there is a good reason why that information should not be shared. Where this is the case the reason why it cannot be transferred will be fully explained to the service user.

8. POLICY SUPPORT

8.1 This Policy should be read in conjunction with the following policies/procedures:

[8] Fraser guidelines

Information Governance Staff Handbook
Data Protection Policy
Information Governance Policy
Information Security Policy
Access to Health Records
Freedom of Information Policy
Information Risk Management Policy
Information Sharing Policy
Records Management Policy
IG Requirements for New Processes and Systems
Environmental Impact Regulations

9. DESIGNATED ACCOUNTABILITY

9.1 The officers accountable for overseeing the implementation of this policy within the Trust are the Caldicott Guardian and the Information Governance Manager.

10. DESIGNATED RESPONSIBLE OFFICER

10.1 The person responsible for the operation, monitoring and review of this policy within the Trust, is the Information Governance Manager.

11. STAFF TRAINING AND AWARENESS

11.1 A training programme will be established to reinforce awareness of the major requirements for all staff within the Trust toward information sharing as part of the Information Governance agenda.

Appendix A - Information Sharing Protocol

Between: (your organisation) _____

And: co-signees of this protocol

This overarching protocol sets out the general principles of Information Governance that the above organisations have signed up to.

It provides a framework for safeguarding the processing of all personal confidential information.

The protocol will be supplemented in some circumstances by individual locally agreed protocols for specific populations/initiatives. These will set out detailed purposes and operational procedures for the sharing of information.

General Principles

1. The Information Governance Toolkit[9] defines the minimum standards for Information Governance for health and social care. Where applicable, each organisation is committed to undertaking, following and complying with the Information Governance Toolkit.

2. Each organisation signing this protocol shall have appointed a responsible officer who will ensure the protection of personal information e.g. Caldicott Guardian or senior manager [10]responsible for data protection.

3. Each organisation signing this protocol will be taking appropriate organisational and technical measures towards compliance with Data Protection Act 1998, Caldicott, ISO 27001 Series of Information Security Standards, Freedom of Information Act 2000 and national guidance and rules around processing personal confidential information and other relevant legislation.

4. Each organisation, where appropriate, is committed to identifying, documenting and risk mitigation of data flows (as required) by the IG Toolkit. A template for documenting information flows is attached.

5. Each organisation is committed to ensuring staff are appropriately trained and comply with organisational policies in relation to Information Governance, including data protection, confidentiality, Caldicott, Information Security, Records Management and Freedom of Information.

6. Organisations signed up to this protocol will promptly notify any other relevant co-signees of this protocol of any Information Governance breach.

7. This protocol will be reviewed in October 2015 (unless any changes to legislation or national policy warrant an earlier review).

Signed by:

Signature	Print name	Date
Caldicott Guardian/authorised officer [11]		

[9] The Information Governance Toolkit is an online performance tool produced by the Department of Health (DH) and hosted by the Health and Social Care Information Centre. It allows NHS organisations and partners to assess themselves against DH information governance policies and standards. https://nww.igt.hscic.gov.uk/

[10] In Health and local authorities, this may be the Senior Information Risk Owner (SIRO). Other agencies may not have these identified roles and, therefore, it will be a senior manager responsible for ensuring compliance with Data Protection.

[11] Same as 2 above

Appendix B - Information flows from organisation “A” to organisation “B”

Flow number/ code	Flow name	**Sender Department and/or borough if not Trust wide**	**Recipient, department or person?**	Purpose	Data Items	**Justified by and date**

Appendix C - Example Information flows from Mental Health Trust to Social Services

Flow number/ code	Flow name	**Sender Department and/or borough if not Trust wide**	**Recipient, department or person?**	Purpose	Data Items	**Justified by and date**
SS1	Violent Incident Report	Risk management	Principal Officer	To inform of violent incidents by service users	1, 4	
SS2	Inter-professional warnings	Risk management	Risk Manager	To warn other professionals of an incident relating to an individual	1, 5	
SS3	Referral	Trust wide	Team	To support care To plan support for service users	1, 3, 4	
SS4	Report	Trust wide	Team	To support care To plan support for service users	1, 3, 4	

Appendix D - Information Flows

Definition of Data Items

No.	Data Item	Definition	
1	Personal	Name Date of birth Next of kin Personal circumstances	Financial information Physical description Gender
2	Personal/ Sensitive	Racial/ethnic origin Religion Trade Union membership	Court Proceedings Criminal convictions Political opinions Sexual life
3	Clinical (Sensitive)	Information relating to physical or mental health or condition	
4	Demographic	Address Postcode Telephone number	Location description Directions
5	Other	Environmental Social	Health Professional
6	Confirmed and/or unconfirmed risk	Risk to self Risk to children	Risk to staff/professionals Risk to others

Appendix E - Information Sharing Frequently Asked Questions

1.	What is personal confidential data (PCD)?	Any information where an individual can be identified, e.g. name, address, date of birth. There are instances where as little as initials and postcode could be enough information to identify someone.
2.	Does client consent have to be in writing?	No. This is not always practical or necessary. A client should be made fully aware of the uses of their data and should be given access to the leaflet "How we use your Information" on first contact with the trust.
3.	Do I have to ask permission to keep personal confidential data (PCD) on a computer?	No. As a responsible health/social services organisation we must keep records and it is our decision to keep them on paper or electronically. We must all keep personal information safely and securely according to legal requirements. (Ask the Information Governance Manager for advice on security of information.)
4.	What if the service users say they do not want me to share their information with other organisations?	Unless it is covered by one of the exceptions see 5.1 of the Information Sharing policy), their wishes must be honoured. It is usually helpful if you explain to them the disadvantages of not sharing but the final decision rests with the individual.
5.	Can I pass information to colleagues in my own team or organisation?	The rules are there to protect the service users. You can pass information to colleagues or other Trust teams on a strictly 'need to know' basis. If they do not need the information to do their job then do not pass the information on.
6.	Can I request information from colleagues in my own team or organisation?	You can request information if you 'need to know' it and be prepared to justify the reason why. If not, you should not request it.
7.	Is there anything else I need to consider before I share?	Make sure the information is accurate and up to date, where appropriate.
8.	How can I be sure that the partner organisation has the same standards of confidentiality and security as my own?	If you have any doubts talk to your line manager and/or the Information Governance Manager before you pass on any information. Organisations that have signed up to the information sharing protocol are committed to the same standards as the Trust.

Appendix F - CHECKLISTS FOR STAFF

SHARING INFORMATION WITH SOMEONE ELSE

1. Does the person requesting the information need it to do their job? □

2. Have you got the service user's consent to pass the information on? □

3. If not, can you justify passing on the information without consent? (See section 5.1 of the Information Sharing policy) □

4. Are you sure the person requesting the information is who they say they are? □

5. Will anonymised or pseudonymised information[12] do? □

6. Do you need to pass on the whole record/file? Try to pass on the minimum information necessary □

WHEN YOU ARE REQUESTING PERSONAL INFORMATION

1. Do you need the information to do your job? □

2. Can you use anonymised or pseudonymised information? □

3. Do you need the whole file/record? If you only need minimum details, or a summary, please only request this. □

[12] Anonymised information is data concerning an individual from which the identity of the individual cannot be determined. Pseudonymised information is data that is anonymised by removing obvious identifiers and adding a new, unique reference. The data is then anonymous to those parties who receive it (e.g. a research team), but still allows the originating party to identify an individual from it.

Appendix G - Definition of Health Professional

Under the Data Protection Act 1998 “Health Professional” means any of the following;

a) A registered medical practitioner (a "registered medical practitioner includes any person who is provisionally registered under section 15 or 21 of the Medical Act 1983 and is engaged in such employment as is mentioned in subsection (3) of that section.)

b) A registered dentist as defined by section 53(1) of the Dentists' Act 1984,

c) A registered optician as defined by section 36(1) of the Opticians Act 1989,

d) A registered pharmaceutical chemist as defined by section 24(1) of the Pharmacy Act 1954 or a registered person as defined by Article 2(2) of the Pharmacy (Northern Ireland) Order 1976,

e) A registered nurse, midwife or health visitor,

f) A registered osteopath as defined by section 41 of the Osteopaths Act 1993

g) A registered chiropractor as defined by section 43 of the Chiropractors Act 1994,

h) Any person who is registered as a member of the profession to which the Professions Supplementary to Medicine Act 1960 for the time being extends,

I) A clinical psychologist, child psychotherapist or speech therapist,

J) A music therapist employed by a health service body, and

K) A scientist employed by such a body as a head of department

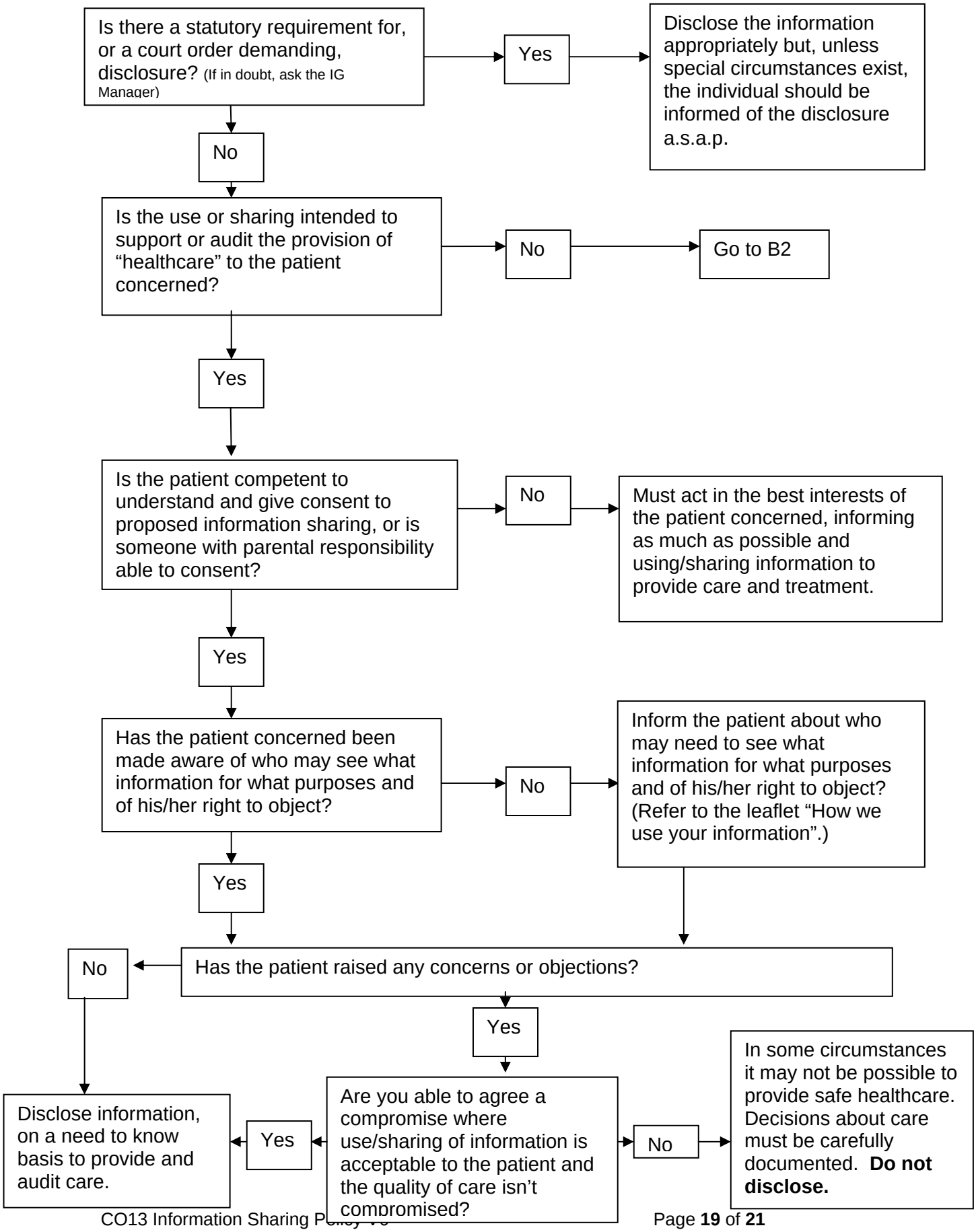
Appendix H - Models for disclosure of confidential information

(The full NHS Code of Confidentiality is available on the Trust intranet in the Governance section under Information Governance or from the Information Governance department if further information is required)

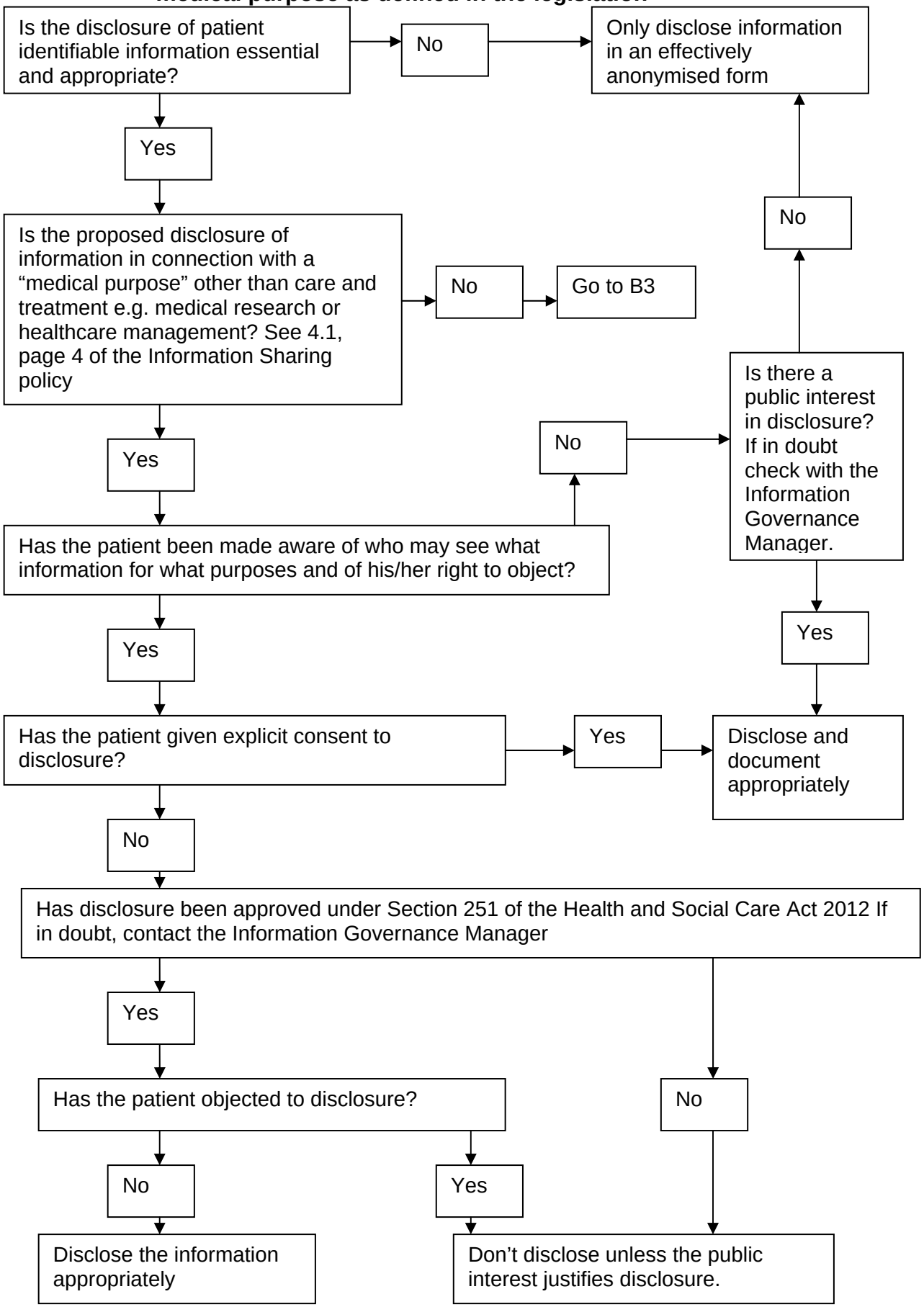
Model B1	disclosures to support or audit healthcare[13]
Model B2	disclosures for other medical purposes (see 5.1)
Model B3	disclosure for non-medical purposes

[13] These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.

B1: Disclosure Model – where it is proposed to share confidential information in order to provide healthcare



B2: Disclosure Model – where the purpose isn't healthcare but it is a medical purpose as defined in the legislation



B3: Disclosure Model – where the purpose is unrelated to healthcare or another medical purpose