Weston Area Health NHS Trust

Gov 20 Confidentiality Policy
v5

Date Approved:	20th March 2018
Date for Review:	1st April 2021
Directorate / Department responsible (author/owner):	Paul Faulkner, Head of Health Informatics
Contact details:	7098
Brief summary of contents	Informs the Trust-wide approach to ensuring the confidentiality of person identifiable information and the responsibilities of staff working for, or on behalf of, the Trust.
Search criteria:	Confidentiality, privacy
Executive Director responsible for Policy:	Director of Finance
Date revised:	February 2018
This document replaces (exact title of previous version):	Confidentiality Policy v4
Title and date of committee/forum/group consulted during development :	Health Informatics Committee
Signature of Executive Director giving approval	
Intranet location:	DMS
Links to key external standards	See appendix 2
Related Documents:	-
Training Need Identified?	None

Version Control Table

Date	V	Summary of changes	Author

Document Amendment Form – minor amendments

No.	Date	Page no	Amendment	Authorised by
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Ten or less minor amendments can be made before the document is revised.

Major changes must result in immediate review of the document

If printed, copied or otherwise transferred from the Trust intranet, procedural documents will be considered uncontrolled copies. Staff must always consult the most up to date version – located on the intranet.

Table of Contents

1. Introduction and purpose

The purpose of this policy is to:

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

This policy links to the Trust's policies covering Information Governance, Data Protection, Records Management, Information Security and employment.

1.1 Principles of Confidentiality

General Principle

Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters in the process of delivering treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the Trust provides, and is seen to provide, a confidential service. One consequence of this is that information that can identify individual patients must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so.

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.

In contrast, de-identifiable information is not confidential and may be used with relatively few constraints.

NHS Code of Practice

The model outlines the requirements that must be met in order to provide patients with a confidential service. Record holders must inform patients of the intended use of their information,

give them the choice to give or withhold their consent as well as protecting their identifiable information from unwarranted disclosures. These processes are inter-linked and should be ongoing to aid the improvement of a confidential service. The four main requirements are:

- PROTECT – look after the patient's information;
- INFORM – ensure that patients are aware of how their information is used;
- PROVIDE CHOICE – allow patients to decide whether their information can be disclosed or used in particular ways.

To support these three requirements, there is a fourth:

- IMPROVE – always look for better ways to protect, inform and provide choice.

Protect

Patients' health information and their interests must be protected through a number of measures:

- Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality;
- Recording patient information accurately and consistently;
- Keeping patient information private;
- Keeping patient information physically secure;
- Disclosing and using information with appropriate care.

Inform Patients Effectively – No Surprises

Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided. Consider whether patients would be surprised to learn that their information was being used in a particular way – if so, then they are not being effectively informed.

In order to inform patients properly, staff must:

- check where practicable that information leaflets on patient confidentiality and information disclosure have been read and understood.
- make clear to patients when information is recorded or health records are accessed;
- make clear to patients when they are or will be disclosing information with others;
- check that patients are aware of the choices available to them in respect of how their information may be disclosed and used;
- check that patients have no concerns or queries about how their information is disclosed and used;
- answer any queries personally or direct the patient to others who can answer their questions or other sources of information;
- respect the rights of patients and facilitate them in exercising their right to have access to their health records.

Provide Choice to Patients

Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. What is very sensitive to one person may be casually discussed in public by another – just because something does not appear to be sensitive does not mean that it is not important to an individual patient in his or her particular circumstances.

Staff must:

- ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of, their care;
- respect patients' decisions to restrict the disclosure or use of information, except where exceptional circumstances apply;
- communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to or restrict the disclosure of information.

Improve Wherever Possible
It is not possible to achieve best practice overnight. Staff must:

- Be aware of the issues surrounding confidentiality and seek training or support where uncertain in order to deal with them appropriately.
- Report possible breaches or risk of breaches using the Trust incident reporting process.

This Trust will offer training to all staff and monitor all reported incidents via the Information Governance Committee.

1.1.1 Practical Compliance Measures

Working Away from the Office Environment
There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry Weston Area Health Trust information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

Taking home/ removing paper documents that contain personal confidential information from Weston Area Health Trust premises is discouraged.

When working away from Weston Area Health Trust locations staff must ensure that their working practice complies with Weston Area Health Trust's policies and procedures. Any removable media must be encrypted as per the current NHS Encryption Guidance.

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location.

Confidential information must be safeguarded at all times and kept in lockable locations.

Staff must minimise the amount of personal confidential information that is taken away from Weston Area Health Trust premises.

If staff do need to carry personal confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of NHS England buildings.

- Confidential information is kept out of sight whilst being transported.

All staff must ensure the above points are considered and remember that they are personally liable for breaches of the Data Protection Act 1998 and their Contract of Employment.

If staff do need to take personal confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.
Staff must NOT forward any personal confidential information via email to their home e-mail account. Staff must not use or store personal confidential information on a privately owned computer or device.

Carelessness
All staff have a legal duty of confidence to keep personal confidential information private and not to divulge information accidentally.

Staff may be held personally liable for a breach of confidence and must not:

- Talk about personal confidential information in public places or where they can be overheard.
- Leave any personal confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents, and
- Leave a computer terminal logged on to a system where personal confidential information can be accessed, unattended.

Steps must be taken to ensure physical safety and security of personal or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons.

Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

Abuse of Privilege
It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 1998.

When dealing with personal confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of Weston Area Health Trust.

If staff have concerns about this issue they should discuss it with their Line Manager or with The Trust's Solicitor or Head of Health Informatics.

2. Scope

2.1 Policy context
Respect for confidentiality is an essential requirement for the preservation of trust.

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 recent review known as 'Caldicott 2', was undertaken in January 2012 to 'ensure a balance between the protection of patient information and the use and sharing of information to improve patient care*".*

The review included a recommendation of an additional principle to the existing 06 principles. These principles to be applied when considering whether such confidential information should be shared.

The Caldicott principles were developed with the aim of establishing the highest practical standards for handling confidential information. The principles apply equally to all personal confidential data whether clinical or non-clinical, manual, computerised, visual, audio recorded or held in a member of staff's head.

The revised list of Caldicott principles:

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient 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.
All NHS organisations and Social Services Departments are required 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, maintain an ongoing advisory role to deal with issues concerning the confidentiality of person identifiable information.

In November 2003 the Department of Health released Confidentiality – NHS Code of Practice which gave more detailed guidance to NHS organisations and staff overseeing the Caldicott principles.

Compliance with the code is monitored via the Information Governance Toolkit which has a section relating to Confidentiality and Data Protection Assurance and links to the Code of Practice and other requirements such as those relating to the Data Protection Act.

The requirements are also explicitly stated within the Healthcare Commission's Standards for Better Health under the C13 core standard which sets out the following requirements:
Healthcare organisations have systems in place to ensure that
….appropriate consent is obtained when required for all contacts with patients and for the use of any patient confidential information;
….staff treat patient information confidentially, except where authorised by legislation to the contrary

2.2 Local Context

The Trust provides services across a number of sites. In providing these services the Trust works closely with the Local Authority, other local NHS Trusts, Clinical Commissioning Groups, Community Partnerships and General Practices. The Trust needs to share information from time to time but irrespective of where, how, with or to whom else the Trust 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 Trust.

2.3 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 personal confidential and de-identifiable information with which the Trust must comply.

- Key additional legislation and guidance includes:
- Data Protection Act 1998
- Crime and Disorder Act 1998
- Human Rights Act 1998

- Freedom of Information Act 2000
- Child Protection Act 2004
- Privacy and Electronic Communications Regulation 2003
- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations 2018

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

The Trust and all staff who work for, or on its behalf, are subject to a Common Law Duty of Confidentiality. All Trust 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.

This policy sets out the requirements to staff to ensure patient confidentiality and patients rights are protected.

3. Explanation of terms

"Confidentiality" can be generally defined as 'when personal and/or sensitive 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.' The information may be held manually, in an electronic format (such as data, video or audio) or in a member of staff's head. It applies equally to both written information and visual information such as a photograph.

4. Roles and Responsibilities

The key responsibilities in the Trust are as follows:

- Senior Information Risk Owner - the Board level responsibility for this role belongs to the Director of Finance.
- Caldicott Guardian - the Medical Director acts as Caldicott Guardian for the Trust.
- Monitoring Committee – the Information Governance Committee is responsible for monitoring the systems designed to ensure compliance with this policy. This Committee in turn reports to the Health Informatics Committee.
- Individual responsibility – all Trust staff have a responsibility to protect the confidentiality of person identifiable information in line with the principles set out in this policy and report any breaches in line with the Trust's incident reporting procedure.

5. Dissemination

Keeping Patients Informed

Patients are kept informed about the Trust's position on the use of patient information through its leaflets.

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, reported incidents and notified or potential legal claims.
- Give opportunity to staff for continual personal and professional improvement through further training
- Statistical analysis.
- Medical or health services research.

All leaflets and information can be provided in a different language or format, in order to meet the special needs of the service user, in line with the Trust's Accessibility Policy. Where a more detailed explanation of the uses to which the information may be put is required the service user should be asked to contact the Patient Advice & Liaison Service in the first instance.

6. Implementation

To meet confidentiality requirements of service users, carers and staff the Trust has the following policies, procedures and/or processes in place.

- Record Keeping Policy
- Data Protection Policy
- Electronic Patient Record (EPR) Policy
- Registration Authority (RA) Policy
- Information Security Policies
- Inter-Agency Information Sharing protocol and underlying agreements (Information Sharing & Data Transfer)
- Disposal and Destruction of Sensitive Data
- Contract of employment - Confidentiality clause
- Electronic Communications Policies (e-mail, internet, network security)
- Home/Remote Working Policy

The list is not exhaustive but these represent the key policies and procedures that are in place. The current list can be found on the Trust Intranet /DMS.

All staff throughout the Trust 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.

7. Monitoring Compliance and Effectiveness

The Health Informatics Committee will oversee the performance of this policy by instigating audits if appropriate and monitoring incidents and complaints at its regular meetings.

8. Staff compliance statement

All staff must comply with the Trust-wide procedural document and failure to do so may be considered a disciplinary matter leading to action being taken under the Trust's Disciplinary Procedure. Actions which constitute breach of confidence, fraud, misuse of NHS resources or illegal activity will be treated as serious misconduct and may result in dismissal from employment and may in addition lead to other legal action against the individual concerned.

9 Equality and Diversity statement

The Trust aims to design and implement services, policies and measures that meet the diverse needs of users of our services, population and workforce, ensuring that none are placed at a disadvantage over others.

Equality Impact Assessment Screening Tool

To be completed for any procedural document when submitted to the appropriate committee for approval.

		Yes/No	Rationale
1	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No	
4	Is the impact of the policy/guidance likely to be negative?	No	
5	If so can the impact be avoided?	No	
6	What alternatives are there to achieving the policy/guidance without the impact?	No	
7	Can we reduce the impact by taking different action?	No	
8	Actions identified following screening process	None	

9	Screening identified a full impact assessment.	No

If you have identified a potential discriminatory impact of this policy/procedure, please refer it the appropriate Director in the first instance, together with suggested actions required to avoid/reduce this impact. For advice in respect of answering the above questions, please contact the H.R Department. For advice on completion of this form please contact the Governance Team.

Appendix 1 - Confidentiality Do's and Don'ts

Do's

1. Do safeguard the confidentiality of all personal confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of Weston Area Health Trust.
2. Do clear your desk at the end of each day, keeping all portable records containing personal confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
3. Do switch off computers with access to person-identifiable or business confidential information, or put them into a password protected mode, if you leave your desk for any length of time.
4. Do ensure that you cannot be overheard when discussing confidential matters. Do challenge and verify where necessary the identity of any person who is making a request for personal confidential information and ensure they have a need to know.
5. Do share only the minimum information necessary.
6. Do transfer personal confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.
7. Do seek advice if you need to share personal confidential information without the consent of the patient/identifiable person's consent, and record the decision and any action taken.
8. Do report any actual or suspected breaches of confidentiality.
9. Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

1. Don't share passwords or leave them lying around for others to see. Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
2. Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
3. Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix 2 - Legislative Context

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 is available in each agency.

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 that “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)
The Children's Act 2004

Caldicott 2 Report
Child Protection

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.