Confidentiality Code of Conduct
(N-061)

Version Number:	V7.06
Author (name & job title)	Karen Robinson, Information Governance Officer
Executive Lead (name & job title):	Hilary Gledhill, Nursing Director
Name of approving body:	Audit Committee
Date full policy approved:	July 2021 (v7.03)
Date Ratified at Trust Board:	N/A (minor amends)
Next Full Review date:	March 2026

Minor amendments made prior to full review date above (see appended document control sheet for details)	
Date approved by Lead Director:	*IG Group – 6 March 2023*
Date EMT as approving body notified for information:	*March 2023*

Policies should be accessed via the Trust intranet to ensure the current version is used

Contents

1. PURPOSE OF THE CODE

All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection legislation and, in addition, for health and other professionals through their own professional Code of Conduct.

This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. Disclosures and sharing of personal identifiable information is governed by the requirements of Acts of Parliament and government guidelines. It should be noted that employees also come into contact with unidentifiable information which should also be treated with the same degree of care e.g. business in confidence information.

This Code applies to all employees of the Trust, including all staff seconded to the Trust, contract, voluntary, temporary and agency staff and other people working on Trust premises. This includes members of staff with an honorary contract or paid an honorarium.

The principle behind this Code of Conduct is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's security systems or controls in order to do so.

Any breach of the Common Law Duty of Confidence, UK General Data Protection Regulation or Data Protection Act 2018 with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with Trust policy will be viewed as gross misconduct and may result in serious disciplinary action being taken, up to and including dismissal. Employees could also face criminal proceedings.

This Code has been written to meet the requirements of:

- Common Law Duty of Confidence
- NHS Trusts and Primary Care Trust (Sexually Transmitted Diseases) Directions 2000
- The Computer Misuse Act 1990
- The Copyright Designs and Patents Act 1988
- The Data Protection Act 2018
- UK General Data Protection Regulation (Keeling Schedule)
- The Human Rights Act 1998
- The Mental Capacity Act 2005

This Code has been produced to:

- protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements.
- make staff aware that confidentiality is not breached when data is shared with other health care professionals for the purposes of direct care.

2. ROLES AND RESPONSIBILITIES

2.1. Chief Executive

The Chief Executive has overall responsibility for Confidentiality within the Trust.

2.2. Senior Information Risk Owner will:

- Chair the Information Governance Group.
- Represent confidentiality and security issues at Trust Board level.

- Oversee the development of an Information Security and Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- Take ownership of risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.
- Review and agree action in respect of identified information risks.
- Ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Provide a focal point for the resolution and/or discussion of information risk issues.
- Ensure the Board is adequately briefed on information risk issues.

2.3 Deputy Director of Finance

- Deputise for the Senior Information Risk Owner as required.

2.4 Caldicott Guardian will:

- Act as the 'conscience' of the Trust regarding confidentiality, and ensure that the Trust satisfies the highest practical standards for the handling of patient information, both within the Trust and data flows to other NHS and non-NHS organisations.
- Ensure that there is a framework enabling Caldicott principles to be reflected in Trust's policies and procedures for the management and use of personal information.
- Be a member of the Information Governance Group and participate in line with the terms of reference for that group.
- Fulfil the responsibilities as stipulated in the Caldicott and Data Protection Policy and Information Governance Policy.
- Supports the Information Governance Team in the development of information sharing protocols.
- Offer support and advice as required to the Information Governance Team on matters relating to confidentiality and patient information.
- Deputise for the Chair of the Information Governance Group.
- Agree and review policies regarding the protection and use of personal information.
- Agree and review protocols governing the disclosure of personal information to partner organisations.
- Make the final decision on issues that arise regarding the protection and use of personal information.

2.5 Deputy Director of Nursing

- Deputise for the Caldicott Guardian as required.

2.6 Data Protection Officer

The Data Protection Officer will:

- Provide support, advice and assurance of data protection compliance across the Trust.
- Maintain expert knowledge of data protection law and practices and how they apply to the business of the Trust.
- Be involved properly and in a timely manner in all issues relating to data protection.
- Support programmes of work from the beginning to ensure that data protection is addressed by default and in the design of new systems and information processes, ensuring the completion of data protection impact assessments (DPIA) when necessary and consulting with the ICO where the proposed processing is high risk.
- Be available to be contacted directly by data subjects.
- Develop and advise senior management on the development and establishment of policies, procedures and other measures to ensure compliance with the data protection legislation.
- Monitor compliance with these measures and provide reports to the highest management level.
- Be the first Trust point of contact for the Information Commissioner's Office and co-operate

with any matter relating to data protection compliance including breach management.

2.7 Information Governance Team will:

Provide advice and guidance in relation to compliance with the Code.

2.8 Employees, contract and agency staff and other people working on Trust premises

All employees, including all staff seconded to the Trust, contract, voluntary, temporary and agency staff and other people working on Trust premises have a duty to comply with the Confidentiality Code of Conduct. This includes members of staff with an honorary contract or paid an honorarium.

Members of staff should also follow the Code of Conduct issued by the professional body to which they are affiliated.

At the start of employment, all staff must sign the confidentiality agreement on page 21.

3. DATA COVERED BY THE CODE

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. Confidential information includes:

3.1. Patient information

Identifiable information includes:

- Patient's surname, forename, initials, address, post code, date of birth, sex, telephone number.
- Pictures, photographs, videos, audio-tapes or other images of patients.
- NHS number, NI number and local patient identifiable codes.
- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

3.2. Staff Information

Personal data about staff relating to their employment with the Trust

3.3. Business sensitive information

Information which, if compromised through alteration, corruption, loss, misuse or unauthorised disclosure, is likely to: -

- adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

3.4. Sensitive information

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding sexually transmitted diseases, HIV and termination of pregnancy).

3.5. Formats
The Code covers all the above information regardless of the format.

It includes:-
- Paper Records
- Electronic records
- Removable media e.g. CDs, DVDs, optical discs, external hard-drives, USB Memory sticks (also known as pen drives or flash drives), Media card readers, embedded microchips (including Smart Cards and SIM cards), MP3 players, digital cameras, audio tapes, visual images (e.g. photograph) and media cards.

4. PROTECTING INFORMATION

Patients' health and social care information and their interests must be protected through following measures.

4.1. Storage of Confidential Information
Paper-based confidential information should always be kept locked away and preferably in a room that is locked when unattended.

Permanent storage of confidential information must be saved in to a secure folder on the Trust network or clinical system. Confidential Information must only be saved on the local hard drive (C: Drive) of laptop computers temporarily for mobile access.

Personal/business sensitive data must only be stored on Trust encrypted devices.

All portable devices e.g. laptops, tablets and smartphones must be encrypted and kept secure. Such devices must be procured through IT Services/Procurement to ensure they meet the Trust's encryption requirements.

Removable media (as detailed in 3.5) must be encrypted, must not be the only source of the information (i.e. the information must also be stored in a secure folder on the Trust network) and only used for secure transportation (i.e. not for routine work). Such media must be kept secure and not be identified as the property of the NHS. The password to the media must not be written down.

Removable media must only be purchased and installed by the IT Service Desk. Non-Trust owned removable media devices must not be used to store or transfer any confidential information. Each user of such media is responsible for the appropriate use and security of data stored on the media.

If removable media is used (as outlined in Section 3.5) then the media must be encrypted and kept in locked storage. Unencrypted electronic media must not be used to transport personal data.

4.2. Use of Internal and External Post
All correspondence containing personal information should always be addressed to a named recipient and department.

All mail must be sent in a securely sealed new envelope, marked confidential. A return address of "Chief Information Officer, Humber Teaching NHS Foundation Trust, Trust HQ, Willerby Hill, Willerby HU10 6ED" should be used.

External mail containing personal information about more than 20 individuals or business sensitive information or detailed sensitive personal information such as case notes, must be sent by special delivery or by NHS courier.

Prior to sending any information to a patient's home address, confirm the address against the address recorded on a Trust system such as Lorenzo or SystmOne.

Double check the mail is addressed correctly for all handwritten or typed addresses before posting.

Check all enclosures placed into an envelope are relevant to the recipient before sealing the envelope to send.

Original Health/Social care records should not be transferred outside the Trust. If a client moves to another area the Medical Records Department will send a copy of the notes on request by special delivery.

Electronic media e.g. CDs used to transport personal data must be encrypted and sent by recorded delivery or by NHS Courier. The encryption key must not be included with the CD. Further advice is available from the IT Service Desk on telephone: 01482 477877.

Further guidance and a flow chart is available in the Safe Haven Procedure.

4.3. E-mailing information

NHSmail provides of secure way of sending personal data/business sensitive information to other NHSmail users by email and Instant Messaging. It is one of a number of Government secure email systems. It connects securely to all of them allowing NHSmail users to share information confidently and securely with their users.

Emails can be sent securely to the following domains without any further action or protection, other than ensuring you have correct recipient:

- nhs.net
- gov.uk (no longer needs to be gsi.gov.uk, gcsx.gov.uk)
- cjsm.net
- pnn.police.uk
- mod.uk
- parliament.uk
- a domain accredited to DCB1596 Secure Email Standard (click here for list)

All personal data/business sensitive information sent outside of these domains must have [secure] in the subject heading. This includes to nhs.uk email addresses and nhs.scot email addresses.

Before using the NHSmail encryption feature:

- ensure that the recipient is expecting it and ready to handle the contents appropriately.
- send the recipient the Accessing Encrypted Email Guide for non-NHSmail users so that they can register for the service.
- send an encrypted email to the recipient with [secure] detailed in the subject heading of the email. At this stage, the email should not contain any personal/business sensitive data. The recipient will then be prompted to register with the encryption service.

Once the recipient has confirmed registration via an encrypted reply, personal data/business sensitive data can then be emailed. The email must still have [secure] in the email heading. Further information can be found at Encryption Guide for NHSmail. The following Guide may also be provided to the recipients of encrypted mail.

It is possible to revoke access to an encrypted email sent using [secure] by following the Encryption Guide for NHSmail and changing the message status from "Active" and "Revoked". This function is not available when the email is sent from a shared mail box.

This method should also be used when communicating by email with a patient/advocate. This must be with the explicit consent of the patient, see Section 3.10 Electronic Communications and Internet Acceptable Use Procedure.

Any breach of confidentiality resulting from using e-mail for personal identifiable data will be investigated and you are responsible for showing why any of the following guidelines may have not been applied. Messages containing personal data sent to the wrong recipient will be classed as a breach of confidentiality even if it is another NHS employee.

Security measures

- Make sure you have the correct recipient. If you are unsure, send a test email or ask the recipient to email you before sending any personal data.
- Mark the message appropriately in the subject line .e.g. "confidential" or "business sensitive" and select "confidential" in the Sensitivity section in the Message Options.
- Limit the number of recipients of the message to as few as possible.
- Limit the amount of data to only that which is needed for the purpose it is being sent e.g. use a unique identifier or initials instead of the person's name.
- Manually select recipients from the address book and confirm their identity by checking the properties.
- Change the address book view to the Humber Teaching NHS Foundation Trust address list. This will avoid the chance of sending an e-mail to another employee in another NHS organisation with the same name.
- Send to e-mail addresses that are person specific unless the e-mail can be dealt with by any member of the team reading the e-mail. Be aware that e-mail can be forwarded by the initial recipient to third parties against your wishes or by accident.
- Include a note to say that the receiver of patient identifiable data is responsible for the security and confidentiality of that data and must not pass it on to anyone else, via any method, who does not have a justified 'need to know'.
- Where there is a more formal method for the communication of information, such as 'web-based' referral system then that must be used.
- If you allow 'delegate' access to other people to your inbox, consider whether they need to see any personal data you receive.
- Anonymised information can be sent to non-secure email addresses, see Glossary of Terms for definition of anonymised.
- When in receipt of personal data remove it from your e-mail system as soon as possible and file it appropriately, either electronically or on paper.
- Review any attachments and make sure all are relevant to the recipients. Attachments containing confidential information not intended for disclosure should be sent separately from general attachments intended for dissemination.
- The file name for confidential attachments should include the word confidential at the beginning.

For further information, please see Electronic Communications and Internet Acceptable Use Procedure.

4.4. Telephone enquiries

Information should only be given over the telephone if you are confident of the identity of the caller. If you are not, you should always take a number, verify it independently and call back. When speaking to a patient or carer on the telephone, confirm the caller's identity or ring back.

Always check whether they are entitled to the information they request. Information about patients should only be released on a need-to-know basis. If in doubt, check with your line manager.

If you receive suspicious queries regarding other members of staff asking about whereabouts, base or personal information, then please treat with caution, take contact details of the caller and either verify that it is an authorised person or pass the details to the individual concerned.

4.5. Disposal of information

When disposing of hand written or printed person-identifiable information, confidential, or business sensitive information, always use 'confidential waste' sacks/shredders. If possible, confidential waste should be shredded at source using a local cross cut shredder and then treated as waste paper.

Confidential waste bags must be stored in locked areas not accessible to the public.

Removable media containing confidential information can be physically destroyed using a shredder. Any other removal media requiring disposal should be hand delivered to the IT Service Desk for secure disposal.

Computer files with confidential information no longer required must be deleted from both the PC and the server if necessary. Computer hard disks are destroyed/disposed of by the IT Services. Please contact the IT Service Desk for further information on 01482 477877.

4.6. Passwords and Smartcards

Personal passwords issued to or created by employees should be regarded as confidential and those passwords must not be communicated to anyone.

- Passwords should not be written down.
- Passwords should not relate to the employee or the system being accessed.
- Passwords should not be shared with colleagues.
- Password should contain numbers and symbols to make them harder to guess.
- If compromised, change your password as soon as possible.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported, via your line manager, using Datix. This must also be reported to the Senior Information Risk Owner. Such breaches of security may result in disciplinary action and may also be regarded as a contravention of the Computer Misuse Act 1990, Data Protection Act 2018 or UK GDPR.

Never share your smartcard and keep it secure at all times. A lost smartcard must be reported to the IT Service Desk as soon as possible.

4.7. Working away from the Trust

Manual Records

Taking personal/business sensitive information away from Trust premises is a risk and should only be taken when absolutely necessary. Personal data includes patient and staff information. See section 11.1 for full definitions.

If you need to take personal/business sensitive information away from the Trust, the following requirements need to be followed.

- Ensure you have authority to take the information. This will normally be granted by your line manager. Authorisation will only be granted when there is an operational requirement for the information to be taken away. For example, only health and social care records required for patients being seen in the community can be removed. Ideally, records should not be removed for general administration purposes, e.g. writing reports.
- If you are taking manual health records, please ensure there is a record that you have these records, where you are taking them and when they will be returned.
- Information must be removed for the minimum amount of time possible.
- Only take the minimum information required for the authorised purpose.
- The information must be stored and carried in a secure case (zipped and locked). Information must not be carried 'loosely' as this increases the risk of dropping them and losing something.
- The secure case must be stored in the locked boot of the car or carried on your person while being transported from your work place to your home. Such information must not be left overnight in a locked boot.
- Secure cases must never be visible in the boot of the car.
- Health records must only be taken home if the health or social care professional is not returning to their base after the working day or the records are required for the next working day. This must be with the prior agreement of the team manager.
- Health records must not be taken home for the purpose of delivering them to another base.
- Remember you are bound by the same rules of confidentiality whilst away from your place of work as you are when you are at your desk.
- When information is in the home, you have personal responsibility to ensure that it is kept secure and confidential. This means that other members of your family and/or your friends/colleagues must not be able to see this information or have access to it. The information must remain in the secure case.

Electronic information

Laptop and mobile devices are vulnerable to theft. Trust devices must never be left unattended and must be stored in locked boot whilst in transit. Such equipment must never be left overnight in an unattended car.

Loss or theft of a device must be reported immediately to the IT Service Desk (01482 477877 – available 24/7) and the incident logged on Datix.

If you take home unidentifiable information/non business sensitive on any removable media outlined in Section 3.5, you must ensure that if you are putting this information onto your own PC that you take the information off again when you have finished your work.

Computerised person-identifiable information or business sensitive information must only be stored on encrypted Trust equipment e.g. a Trust encrypted laptop, a Trust encrypted memory stick.

Personal or business sensitive information stored on a Trust encrypted memory stick must be not transferred on to a non-Trust device.

Non-personal or non-business sensitive information, for example, a power-point presentation or report can be transferred onto a non-Trust device, PC or laptop.

Do not open attachments in e-mails containing personal data/business sensitive information on equipment that doesn't belong to the Trust, even via the secure NHSmail web app.

Smart devices which use voice-controlled virtual assistants such as Alexa and Google Assist should not be used in your work environment. Such devices (e.g. smart speakers and smart watches) can record information and should not used in a room where patient or staff details or business sensitive data is discussed.

4.8. Personal Use of Social Media

When using social media in a private capacity, employees must not: -

- Post comments on social network sites, discussion forums, blogs etc. which contain: any personal identifiable information (patient and staff data), inappropriate comments or personal criticism of colleagues or patients, names of other staff without their permission, criticism of the organisation, statements by or on behalf of the organisation, comments that may bring the organisation into disrepute, information about work related issues, information or language that could be considered bullying, intimidating, harassment or discriminatory against any individual.
- Identify the Trust as your employer on social network sites used for a personal use. This does not apply to professional networking sites such as LinkedIn.
- Take any images or recording of patients on your personal phone/camera or any other personal equipment. Any recordings taken using Trust equipment must gain appropriate consent and follow the Trust's Procedure on Photographing, video and audio recording of patients, carers and members of staff.
- Build or pursue relationships with patients.
- Steal personal information or using someone else's identity.

Staff must ensure that their use of social media complies with their professional Codes of Conduct and the Trust's Social Media and Website Policy.

4.9. Abuse of privilege

It is strictly forbidden for employees to look at any information for their own personal use, for example, information relating to, their own family, friends or acquaintances unless they are directly involved in the patient's clinical care or with the employees administration on behalf of the Trust. Action of this kind will be viewed as a breach of confidentiality and will result in disciplinary action.

Additionally, staff have no personal or informal right to access their own medical and confidential record. This would be considered a breach of contractual obligations and would be subject to disciplinary action by the Trust. Staff wishing to exercise their right of access will need to make a subject access request following the Access to Health Records Policy or the Data Protection for Employment Records Procedure, depending on the records required.

If you have concerns about this issue please discuss with your line manager.

Staff must ensure that they document why they have accessed an electronic record when it is not obvious within the record itself e.g. a referral to the team, a clinical entry or document uploaded to the record.

4.10. General

- Do not talk about patients in public places or where you can be overheard.
- Do not leave any medical records or confidential information lying around unattended.
- Make sure that any computer screens, or other displays of information, cannot be seen by the general public, or others when working from home.
- Use the secure print facility when printing personal/business sensitive information to network printers and copiers.

4.11. Security incident

A Security Incident is any event that has or could: -

- Cause an unauthorised disclosure of confidential, personal or business sensitive information.
- Put the integrity of a computer system or data at risk.
- Put the availability of the system or information at risk.
- Have an adverse impact e.g. embarrassment to the NHS.

All incidents or information indicating a suspected or actual security breach should be reported, via your line manager, using Datix, as soon as you become aware of the incident.

Serious incidents must also be reported to the Senior Information Risk Owner. The Information Governance Team will assess and grade the incident in accordance with the NHS Digital Guide to the Notification of Data Security and Protection Incidents.

Incidents reportable to the ICO will be recorded on the DSP Toolkit within 72 hours. Approval from the Senior Information Risk Owner, Caldicott Guardian and Data Protection Officer will be sought prior to reporting.

4.12. Further information

Further details about protecting information can be found in: -

- Safe Haven Procedure
- Information Security and Risk Policy
- User responsibilities for passwords
- Selecting a domain password
- Electronic Communications and Acceptable Use Procedure

5. COPYING OF SOFTWARE

All computer software used with the Trust is regulated by license agreements. A breach of the agreement could lead to legal action against the organisation and/or the offender (member of staff).

It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use. This would be a breach the license agreement.

Employees must not load software onto their computer before first seeking advice/agreement from the IT Service Desk.

6. INFORMING PATIENTS

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. Staff should 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.

The patient privacy notice (http://intranet.humber.nhs.uk/directorates/ig-leaflets.htm) should be given to all new patients when we first collect their information. In order to inform patients properly, staff must:

- Check where practicable that “Patient Privacy Notice (short version) has been read and understood.
- Make clear to patients when information is recorded or health records are accessed.

- Make clear to patients when staff are or will be disclosing information with others.
- Inform patients about circumstances when confidentiality may be overruled.
- Check that patients are aware of the choices available to them in respect of how their information may be disclosed and used.
- Communicating effectively with patients to help them understand. Please contact the Information Governance Team if you require the leaflet in a different format or language.
- Informing patients about the importance of providing accurate information.
- Giving patients the opportunity to check information held about them.
- Encouraging patients to inform the Trust if any of their details have changed.
- 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 the Information Governance Team who can answer their questions.
- Respect the right of patients and facilitate them in exercising their right to have access to their health records.

Further details can be found in the NHS Confidentiality Code of Practice.

7. PROVIDING 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, see Section 9.4 and 9.8
- 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
- Ensure that patient understands and agrees to any disclosures of sensitive information (see 3.4) to support their care.
- Note any restrictions placed by the patient in their medical record and on their computer record, see Policy for patient objections to the creation or use of their health record

Further details can be found in the NHS Confidentiality Code of Practice.

8. IMPROVE WHEREVER POSSIBLE

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.

9. USE AND DISCLOSURE OF PATIENT INFORMATION

The following section deals with the uses and disclosures of patient information, including the issue of consent.

Prior to disclosing information, staff must ensure that the information is accurate and up to date, confirming patient details against the Trust systems such as Lorenzo or SystmOne.

Bulk transfers of data (50 records or more) require authorisation of the Senior Information Risk Owner.

Access to patient records by external organisations (e.g. Commissioners, Health Watch and Governors) must only be given with the approval of the Caldicott Guardian. The request for authorisation must be submitted to the Information Governance Team in the first instance. The request should detail: -

- The reason and purpose for the request, including any project documentation.
- Details of the information required and justification for each personal data identifier. (For example name, NHS number, dob, age, post code, partial postcode etc.)
- The legal basis for the request, for example: the consent of the patient, Section 251 NHS Act 2006 approval. Any consent form must accompany the request.
- How patient objections will be dealt with.
- How any information obtained by the external organisation will be stored and the retention period.
- How the information will be destroyed.
- Any further disclosures of the information e.g. anonymised published results.

The IG Team will review the request and submit it to the Caldicott Guardian for authorisation, highlighting any information governance issues. The request will be logged on the Caldicott Function log. The IG Team will feedback the Caldicott Guardian's decision to the project lead. Access must only be given to the records once this is received.

Further information about the use and disclosure of information can be found in:
- Humber Information Sharing Charter. This is supported by specific information sharing agreements click here
- Clinical Audit and Service Evaluation Policy and Procedure

9.1. The Caldicott Principles

The use and disclosure of patient information must comply with the following principles: -

- Justify the purpose(s) for using confidential information.
- Use confidential information only when it is necessary.
- Use the minimum necessary confidential information.
- Access to the confidential information should be on a strict need to know basis.
- Everyone with access to confidential information should be aware of their responsibilities.
- Comply with the law (for example the Data Protection Act 2018 and common law duty of confidence).
- The duty to share information can be as important as the duty to protect patient confidentiality.
- Inform patients and service users about how their confidential information is used.

9.2. Direct Care

Information may be shared to provide the patient with care and treatment without their explicit consent, providing that the patients have been informed of: -

- the use and disclosure of their information associated with their health care, see Section 5; **and**
- the choices that they have and the implications for choosing to limit how information may be used or shared, see Section 9.4 for limitations.

You should share relevant information that is necessary to support individual care. This includes with other health organisations, GP practices, care homes, prison health care and private health care providers. This may be necessary to support a specific issue or to support a transfer of care. Wherever possible, patients should be made aware of the disclosure. All information must be shared securely following the security measures in Section 4.

9.3. Non-direct care purposes

Explicit consent is required for any purpose other than the provision of healthcare, unless anonymised information is being used/disclosed.

Explicit consent is required before sharing information with a carer or significant other. The patient's decision should be recorded on the Information Sharing Decision Record. If a patient does not agree for their information to be shared, this will be respected unless there is an overriding public interest, see 9.8.1. This does not prevent staff from listening to carers or from providing non-confidential information e.g. signposting support organisations. See information-sharing-with-carers-and-significant-others-sop.htm (humber.nhs.uk) for further information.

Explicit consent is also required for the patients sharing preferences on SystmOne, see edsm-sop.htm (humber.nhs.uk).

Explicit consent should be obtained at the earliest opportunity. In order to gain consent, the patient must be informed of: -

- What information is to be shared.
- Who it is to be shared with.
- The purpose for sharing the information.

It should be made clear to the patient that they have the right to withhold their consent, see 9.4.

Ideally, consent should be sought by the member of staff/team who collected the confidential information. In some circumstances, an organisation requiring information for a further purpose may have already gained consent. A copy of the signed consent should be obtained prior to the release of information.

9.4. Recording explicit consent

Explicit consent should be in writing with a copy given to the individual and a copy placed in the individual's file. If consent is obtained verbally, this should be documented in the individual's file. Wherever possible, a service area should use a standard consent form to record consent.

Clinical audit and research projects requiring explicit consent will retain the explicit consent form with the project documentation.

9.5. Refusal/limitations on consent

Patients do have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential healthcare, subject to certain exemptions, see Section 9.8. They may also limit the consent given. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a patient exercising his or her right to refuse treatment.

In such circumstances staff should: -

- Clearly establish the concerns of the patient and look at whether there is a technical or procedural way of satisfying the consent without unduly compromising care.
- Explore the options for providing an alternative form of care or to provide care through alternative arrangements.
- Assess the options that might be offered to the patient, balancing the risks, staff time and other costs attached to each alternative that might be offered against the risk to the patient of not providing healthcare.

Careful documentation of the decision making process and the choices made by the patient must be included within the patient's record or the explicit consent form that will be included in the patient's record.

Any restrictions placed by the patient must be noted in the medical record and an alert placed on the inside cover of their medical record and on their computer record, see Procedure for patient objections to the creation or use of their health record.

If the patient chooses not to give consent, revokes consent or chooses to limit their consent then they should be informed that this may limit the services that can be provided to them. Patients should be informed that if consent is revoked, it may not be possible to retrieve information already shared. In exceptional circumstances, it will be possible to proceed with the information sharing without explicit consent, see 9.8.

9.6. Patients who are unable to consent

Where a patient is incapacitated and unable to consent, information should only be disclosed in the patient's best interests, and then only as much information as is needed to support their care. Any previously expressed wishes, informed by the views of relatives or carers as to the likely wishes of the patient should be taken into account. If a patient has made his or her preferences about information disclosures known in advance, this should be respected. Decisions to disclose and the justification for disclosing should be noted in the patient's record.

9.7. Reviewing consent

Consent should be reviewed with the patient at any formal review and when the purpose for which the information is to be shared has changed, or the information is to be given to different organisations or individuals than originally agreed with the patient.

Consent forms within Information Sharing Agreements must be reviewed regularly to check that the relationship, the processing and the purposes have not changed.

9.8. Answering patient questions about consent

When seeking explicit consent, patients should be given the opportunity to talk to someone they can trust and of whom they can ask questions. The patient should be given support and explanations about any form that they are required to sign. If the member of staff is unable to answer the patient's questions, the patient should be directed to the Information Governance Team.

9.9. Exemptions to the requirement for consent

There are certain circumstances when personal information given in confidence may be used or disclosed without the patient's consent, these are: -

9.9.1. Over-riding public interest

Personal data may be disclosed to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others. Decisions to

disclose in these circumstances must be made on a case by case basis, justifying that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service.

A record must be made of any such circumstances, so that there is clear evidence of the reasoning used and the circumstances prevailing. Disclosures in the public interest should also be proportionate and be limited to relevant details. It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision making process and the advice sought is in the interest of both staff and the Trust. A decision not to disclose information may also be challenged and must be documented, detailing the justification for not disclosing.

Wherever possible the issue of disclosure should be discussed with the individual concerned and consent sought. Where this is not forthcoming, the individual should be told of any decision to disclose against his/her wishes. This will not be possible in certain circumstances, e.g. where the likelihood of a violent response is significant or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

Consideration should also be given to the disclosure of anonymised information – at least at the outset. For example, if a patient disclosed that Dr X sexually assaulted a patient and the patient does not agreed to be named, the concern may be reported without revealing the identity of the patient. The disclosure may reveal a cluster of complaints or a pattern of behaviour. It should be made clear to the patient that there is a duty to protect the safety of other NHS patients and their identity may need to be revealed in the future. The disclosure of partial information will need to be reviewed by the healthcare worker to ensure that the information given has allowed sufficient action to be taken that is in proportion to the risk.

An example of a disclosure in the public interest is where a patient continues to drive, against medical advice, when unfit to do so. In such circumstances you should disclose relevant medical information immediately, in confidence, to the medical adviser at the DVLA. Confidentiality - GMC (gmc-uk.org)

If you require advice on disclosing information in such circumstances, please seek advice from the Information Governance Team.

The Department of Health supplementary guidance on public interest is available at: Public Interest Disclosures

9.9.2. Legal requirement

Some statutes place a strict requirement on clinicians or other staff to disclose information. Care should be taken however to only disclose the information required to comply with and fulfil the purpose of the law. If staff have reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the patient or another person, they should seek legal advice. Legal and professional obligations that affect the use and disclosure of personal information are detailed on the Department of Health web-site at http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_079616

The courts, including coroner's courts, some tribunals and persons appointed to hold inquiries have legal powers to require that information that may be relevant to matters within their jurisdiction be disclosed. This does not require the consent of the patient whose records are to be disclosed but he/she should be informed, preferably prior to disclosure. Disclosures must be strictly in accordance with the terms of a court order and to the bodies

specified in the order. Where staff are concerned that a court order requires disclosure of sensitive information that is not relevant to the case in question, they may raise ethical concerns with the judge or presiding officer. If, however, the order is not amended it must be complied with.

9.9.3. Care Quality Commission

CQC have legal powers to access information. CQC will inform providers of the legal basis and reasons as to why they require access to or information from medical records. Wherever possible, the patient must be informed about the access to information. If a patient objects, the CQC will take this into account. CQC will only access confidential personal data against the expressed wishes of the patient in exceptional circumstances and will inform the patient of the reasons for doing so.

Only people specifically authorised by CQC are allowed to use these power to access confidential personal information. This authorisation may be printed on the rear of an Inspectors' CQC identity badges, or may be a separate letter or document from CQC.

The CQC Code of Practice on confidential personal information will be followed for any access. Such requests do not require authorisation from the Caldicott Guardian, however, the Caldicott Guardian should be informed wherever possible. During a main CQC Inspection, all requests for data will be submitted to the Trust's CQC Inspection Team. During ad-hoc visits, the request may be direct to the team providing care.

Staff must ensure that a note is be made in the medical record that CQC has accessed the record. Teams should also take a copy of the records CQC have asked to look at and submit these to the Assistant Director of Nursing, Patient Safety and Compliance.

9.9.4. Section 251 NHS Act 2006

Section 251 of the NHS Act 2006 makes it lawful to disclose and use confidential patient information in specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. This does not create new statutory gateways, so the processing must still be for a lawful function, but does mean that the confidentiality obligations do not have to be met, e.g. consent does not have to be obtained. Even where these powers apply however, the Data Protection Act 2018 continues to apply.

The Confidentiality Advisory Group (CAG) provides independent advice to the Health Research Authority regarding applications under Section 251 of the NHS Act 2006. Click here for further information

Data flows which rely on Section 251 approval must apply the National Data Opt-out unless specifically exempt. Please contact the Information Governance Team if you have a data flow that relies on Section 251 approval. Please see Procedure for Patient Objection to the Creation or Use of their Health Record for further information.

9.9.5. Medical Examiners

Medical examiners may request the records of deceased people for independent scrutiny. The sharing of relevant confidential patient information with medical examiners is covered by a Section 251 approval.

9.9.6. Anonymised information

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification. Information that has been de-identified rather than anonymised requires

further agreements before disclosure. See HSCIC - A guide to confidentiality in health and social care available on the NHS Digital website

10. FURTHER INFORMATION

Further guidance regarding confidentiality and patients' consent to use their health records can be found in the Confidentiality: NHS Code of Practice and the supplementary guidance on public interest. Both documents can be found http://intranet.humber.nhs.uk/directorates/information-governance.htm under "Related Downloads".

Further information may also be found in the following policies and procedures available on the Intranet.

- Access to Records Policy
- Caldicott and Data Protection Policy
- Clinical Audit and Service Evaluation Policy and Procedure
- Data Quality Policy
- Electronic Communications and Acceptable Use Procedure
- Humber Information Sharing Charter
- Information Governance Training Procedure
- Information and IT Forensic Procedure
- Information Security and Risk Policy
- Information sharing with Carers and Significant others Standard Operating Procedure
- Photographing, video and audio recording procedure
- Procedure for patient objections to the creation and use of their health record.
- Safe Haven Procedure
- Selecting a domain password
- Social Media and Website Policy
- User responsibilities for passwords

11. MONITORING

The Code of Conduct will be monitored via the associated policies detailed above.

12. CONTACTS

Information Governance Team (Any questions or assistance regarding the Code of Conduct).- hnf-tr.igteam@nhs.net or telephone 01482 477854

IT Service Desk (Technical assistance re viruses, encryption, password protection etc) hnf-tr.itservicedesk@nhs.net or telephone 01482 477877,

Peter Beckwith, Senior Information Risk Owner –peterbeckwith@nhs.net

Hilary Gledhill, Caldicott Guardian – hilarygledhill@nhs.net

Lisa Davies, Head of Information Governance and Legal Services , Data Protection Officer– Lisa.davies14@nhs.net

13. AGREEMENT DOCUMENT

Your personal responsibility concerning security and confidentiality of information (relating to patients, staff and the organisation)

During the course of your time with the Trust, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of the Trust. This condition applies during your relationship with the Trust and after the relationship ceases.

Confidential information includes all information relating to the Trust and its patients and employees. Such information may relate to patient records, telephone enquiries about patients or staff, electronic databases or methods of communication, hand-written notes containing patient information etc. If you are in doubt as to what information may be disclosed, you must check with a manager.

The Data Protection Act 2018 and the UK General Data Protection Regulation regulates the use of computerised information and paper records of identifiable individuals (patients and staff). If you are found to have unlawfully used/accessed confidential information you may face legal action. In addition, if you are found to unlawfully used/accessed confidential information or failed to protect personal data in accordance with Trust policy, you will be subject to the Trust's Disciplinary Procedure.

I understand that I am bound by a duty of confidentiality and I have read and understood this Code of Conduct and the requirements of the data protection legislation detailed in this Code of Conduct.

PRINT NAME:	
SIGNATURE:	
DATE:	

Please retain a copy of this agreement. The original must be forward to the HR Department for inclusion in your record.

Appendix 1 - Document Control Sheet

This document control sheet, when presented to an approving committee must be completed in full to provide assurance to the approving committee.

Document Type	Code of Conduct		
Document Purpose	To ensure that all staff handle personal data in a confidential and secure manner. The Code covers the protection of personal information and the use and disclosure of patient information.		
Consultation/ Peer Review:	Date:	Group / Individual	
list in right hand columns consultation groups and dates ->			
Approving Committee:	Information Governance Group	Date of Approval:	
Ratified at:		Date of Ratification:	
Training Needs Analysis: *(please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)*	The requirements of the Code are covered in all face to face IG training sessions	Financial Resource Impact	There are no financial resource implications of this Code.
Equality Impact Assessment undertaken?	Yes [x]	No [ ]	N/A [ ] Rationale:
Publication and Dissemination	Intranet [x]	Internet [ ]	Staff Email [x]
Master version held by:	Author [x]	HealthAssure [ ]	
Implementation:	*Describe implementation plans below - to be delivered by the Author:*		
	• All staff emailed as part of the MidWeek Global with a link to the procedure.		
Monitoring and Compliance:	Monitoring and compliance with this Code will be via the associated policies and procedures detailed in the Code of Conduct.		

Document Change History:			
Version Number / Name of procedural document this supersedes	*Type of Change i.e. Review / Legislation*	*Date*	*Details of Change and approving group or Executive Lead (if done outside of the formal revision process)*
5.11			
5.12	*Review*	*5/12/11*	*The Code of Conduct has been reviewed and the changes are:-* • *Title changed from "Code of Conduct for employees in respect of confidentiality and information security" to "Confidentiality Code of Conduct".* • *Two additional pieces of legislation referenced in section 1. NHS Trusts and Primary Care Trust (sexually transmitted Diseases Directions 2000 and the Mental Capacity Act 2005.* • *Roles and responsibilities added in line with other policies.* • *Code updated with relevant changes from the Electronic Communications and Internet*

			acceptable use policy and also the Safe Haven Policy. • *Section added to 4.12 regarding social networking* • *Internet and intranet links and contacts updated.* *Reference added to the DoH Supplementary Guidance on disclosures in the public interest.*
6.0	*Review*	*September 2015*	• *Job titles, web links, contacts details, policy names updated.* • *Expanded section 1 and 2.5 to include members of staff with an honorary contract or paid an honorarium.* • *2.3 remove the requirement for the Caldicott Guardian to specifically sign off the Confidentiality and Data Protection components of the IG Toolkit.* • *4.3 additional requirement that personal information must only be faxed in exceptional circumstances when other secure methods are not available.* • *4.4 and 4.9 Updated in line with the Electronic Communications Policy.* • *4.6 and 4.8 updated in line with Safe Haven Policy.* • *4.6 additional requirement that confidential waste bags must be stored in locked areas not accessible to the public.* • *4.10 abuse of privilege includes records about themselves.* • *9 addition to ensure information disclosed is accurate. Also require authorisation for the disclosure of bulk data.* • *9.1 additional Caldicott principle.* • *9.2 link to the EDSM information sharing procedure and information regarding information sharing with carers and significant others.* • *9.8 additional information about de-identified information.* • *Update policy list.*
6.01	*Review*	*Nov 2016*	*4.8 updated inline with Safe Haven Policy wording. 4.1 and 4.8 updated to incorporate further remote working requirements.* *Following the IG Committee, Section 9 updated to incorporate requests from external organisations to access patient data, including a specific section on requests from the CQC. SIRO updated.*
6.02	*Amendment*	*February 2017*	*Access to patient data by external organisations SOP incorporated into Section 9 and Section 9.8.3.*
7.0	*Review*	*September 2018*	*Reference updated to revised Data Protection legislation* *Caldicott Guardian role update inline with latest job description* *Include returned mail address*

			Double checking handwritten/typed addresses. *Email information where possible rather than fax* *Update email section in line with the Electronic Comms Policy.* *Include Smartcard security* *Remove the requirement to store manual information seperately to laptops.* *Staff documenting the reason for accessing electronic records.* *Using secure print for network printers/copiers.* *Update Section 7 when disclosing sensitive information* *Update policy links and contact details.*
7.01	*Update*	*March 2019*	*Update 4.4 on secure email in line with the Electronic Communications and Internet Acceptable Use Procedure*
7.02	*Update*	*September 2019*	*Update 4.1 on Storage of Confidential Information in line with Safe Haven Procedure update.*
7.03	*Review*	*July 2021*	*Removed all references to fax machines. Updated legislation to refer to UK GDPR. Add in references to the Social Media and Website Policy. In Section 1, add a further purpose that confidentiality is not breached when shared for direct care. In Section 2, added in role of DPO. In Section 4.2 add in the requirement to check addresses against the clinical system and to check envelope enclosures before sending. Section 4.3 updated in line with current Electronic Comms Procedure with the addition that it is not possible to revoke access to a [secure] email from a shared mailbox. In section 4.6 advise staff to change passwords asap if compromised and advise staff on the legislation that may be breached if security is breached. In Section 4.7 include advice on Smart Devices. Update 4.9 in relation to staff accessing their own records. Update 4.10 to include when working from home. Update 4.11 to include the grading of incidents and the reporting serious incidents to the ICO in 72 hours. In Section 9.1 update the Caldicott Principles to the latest wording from the National Data Guardian. Expand 9.6 in relation to reviewing consent. Update the Confidentiality Agreement to include unlawfully used/accessed.*
7.04	*Update*	*July 2022*	*9.8.4 expanded to include the application of the National Data opt-out*
7.05	*Update*	*October 2022*	*9..8 expanded to include Medical Examiners requests for confidential information.*
7.06	*Update*	*March 2023*	*9.2 Obtaining patient consent, split in to two sections, direct care and non-direct care purposes. Direct care section expanded to include a range of health organisations who we may share information. Approved virtually by IG Group (6 March 2023).*