NHS

Bolton Clinical Commissioning Group

Secure Transfers of Data Procedure

Policy Number	**IG012**
Target Audience	**CCG staff**
Approving Committee	**CG Chief Officer**
Date Approved	**17th September 2020**
Last Review Date	**April 2020**
Next Review Date	**17th September 2022**
Policy Author	**IG Team**
Version Number	**V5.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	Sept 13	G Birch M Robinson D Sankey	Progress to CCG Executive for approval
1	September 2013	CCG Exec	Approved
1.1	June 2015	IG Team	Reviewed & progress to IM & T Operations Board for approval.
2.0	June 2015	IM & T Operations Board	Approved
3.0	June 2017	IG Team	Reviewed & progress to IM & T Operations Board for approval.
4.0	December 2017	CCG Chief Officer	Approved
4.1	October 2018	IG Team	Reviewed and updated in line with GDPR
4.2	October 2018	IG Board	Approved
5.0	December 2018	CCG Chief Officer	Approved
5.1	April 2020	IG Team	Reviewed and updated

Analysis of Effect completed:	By: M Robinson	Date: Sept 2013

Contents

1. Introduction and Aims 4
2. Scope 4
3. Confidentiality, Integrity & Security 4
4. Definitions 5
5. Responsibilities 6
6. Key Legislation / Guidance relating to secure transfers of data 7
7. Data Security in the Work Environment 9
8. Transfers of Data by Email 10
9. Telephone Disclosures 13
10. Transfers of Data by Post 14
11. Manual transfers of Paper / Hardcopy Documentation 15
12. Transfers of Data to Photocopiers / Printers 15
13. Transfers of Data via Text Message 15
14. Transfers of Data using Portable Devices 16
15. Transfers of Data by the NHS Secure Electronic File Transfer (SEFT) Service 17
16. Transfer of Information to Cloud Storage 17
17. Non Routine Bulk Transfers 17

17. Transfers of Data via Social Media Platforms 17
18. Transfers of Data via Audio Recordings 17
19. Transfers of data via photography and video equipment 18
20. Transfers of Data Overseas 18
21. Disposal / Deletion of data 18
22. Monitoring and Review 19
23. Legislation and related documents 19
24. Links and further information 20

1. Introduction and Aims

1.1. The purpose of this document is to provide guidance to all Bolton CCG (henceforth referred to as “the CCG”) staff on the secure transfers of data / information, specifically where this is personal data and / or business sensitive data.

1.2. When transferring data / information staff need to take into account the nature of the information to be transferred and ensure that it has the necessary protection to ensure its security. This is especially important when information contains personal, confidential or special category data. This procedure sets out different types of transfer and security requirements. However, please seek the advice from the Data Protection Officer / Information Governance (IG) Team if a transfer method is not included here to assess the most secure option for your transfer of data.

1.3. To ensure compliance with GDPR (see Section 6) routine transfers of personal data and business sensitive data must be logged on the CCG’s Data Flow Mapping Register. This then enables the CCG to provide transparency and demonstrate integrity regarding the data flows it processes and how these are transferred securely to ensure that patients and staff trust us to process their data.

2. Scope

2.1. This procedure applies to those members of staff who are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority / honorary contract or work experience the organisation’s policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

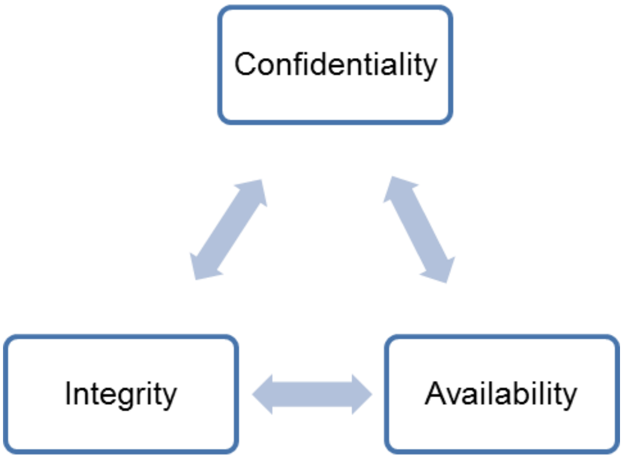
2.2. When information is being transferred from one CCG / location / organisation to another staff must ensure that this is transported securely particularly when this is personal data and / or business sensitive data. This procedure sets out a framework to inform staff who are responsible for transporting routine flows of personal data, special category data, personal staff information, business sensitive and / or commercial in confidence information and any other similar exchanges must adhere to.

2.3. All CCG staff must maintain the confidentiality of personal data when processing this including the transportation of this.

2.4. Please note compliance of this procedure is monitored by confidentiality audits as outlined in the Confidentiality Audit Procedure. These are conducted by the Data Protection Officer Information Governance (IG) Team (see Section 4). The results of these audits are fed back to the IG Board who monitor compliance and take action where necessary.

3. Confidentiality, Integrity & Security

3.1. Data Security can be broken down into three areas: Confidentiality, Integrity and Availability and these are fundamental when transferring / accessing data.



3.2. **Confidentiality** is about privacy and ensuring information is kept confidential and only available to those with a proven need to see it. This data must not be disclosed to others unless a legal statute or patient / public interest applies. It would be unacceptable for a perfect stranger to be able to access personal data from a laptop simply by lifting the lid and switching it on. That's why a laptop should be password-protected and the data on it encrypted when switched off and also when this information is transferred it must be done so following secure transfer processes.

3.3. **Integrity** is about information stored in, for example, a database being consistent and unmodified. Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration. Secure transfer processes such as encryption must be followed when transferring information to ensure this remains secure.

3.4. **Availability** is about information being there when needed. System design must include appropriate access controls and checks so that the information in the system has consistency and accuracy, can be trusted as correct and can be relied on when providing health or care.

4. Definitions

4.1. **Personal Data** - This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

4.2. **Special Category Data** - This is personal data consisting of information regarding: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under GDPR, this now includes biometric data and genetic data.

For more information about special category data please refer to the ICO guide at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

4.3. **Business Sensitive Information**
This is information that if disclosed could harm or damage the reputation or image of an organisation.

4.4. **Personal Confidential Data** - This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special category data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

4.5. **Processing** – This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5. Responsibilities

5.1. **Chief Officer** - has overall responsibility for the implementations of the provisions of this procedure. As the Accountable Officer, they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

5.2. **Caldicott Guardian -** has responsibility for ensuring secure transfers of data procedures are in place throughout the organisation, particularly where the data concerns patients. The Information Governance (IG) Team along with the Data Protection Officer (DPO) / will monitor and investigate any secure transfers of data breaches and seek guidance from the Caldicott Guardian when a breach concerns patient data.

5.3. **Senior Risk Information Officer (SIRO)** - with support of the Information Asset Owners, CCG Executive Directors / Heads of Service / Line Managers has responsibility for ensuring that all staff are aware of the secure transfer of data / information procedures and the importance of understanding the key information assets within their departments and the type of data flowing in and out.

Data Protection Officer (DPO) - is the person that has been assigned the responsibilities set out in the GDPR, such as monitoring and assuring CCG compliance with Data Protection legislation, therefore will ensure that staff are provided with advice and guidance, via this procedure and other associated IG policies on how to ensure data is transferred securely, adhering to the GDPR Principle f – the security principle.

5.5. **Associate Directors / Line Managers** have responsibility for ensuring that all staff are aware of and understand this procedure

5.6. **Employees** - have a responsibility for ensuring the information is handled, used, stored and shared confidentially and appropriately. If in doubt individuals should seek guidance from their line manager in the first instance, the IG Team or the DPO.

6. Key Legislation / Guidance relating to secure transfers of data

6.1. A number of acts and guidance dictate the need for secure transfer arrangements to be set in place; they include (but are not restricted to):

- General Data Protection Regulation (GDPR) 2016
- Data Protection Act (2018)
- National Data Guardian Data Security Standards

6.2. Article 5 of GDPR sets out seven key principles, these principles, in particular Art 5(f), along with the 10 Data Security Standards (detailed below) are integral to the safe and secure transfer of information.

6.3. General Data Protection Regulation 2016 (GDPR) / the Data Protection Act May 2018

6.4. The GDPR and the Data Protection Act 2018 (DPA) are the data protection legislations that sit side by side and provide a legal framework protecting individual's personal data. Any organisation that process personal data must ensure they comply with the legislation to avoid investigation by the Information Commissioner's Office (ICO).

6.5. The aim of the GDPR is to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and the rules enabling the free movement of Personal Data.

6.6. GDPR Principles

All staff must adhere to the principles of the GDPR when processing personal and / or special category data and demonstrate compliance with these.

Article 5 of GDPR sets out seven key principles which lie at the heart of this data protection regime. Principle (f) is also referred to as the 'security' principle and includes ensuring the secure transfer of information.

Article 5 of the GDPR states that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

The seventh principle relates to "accountability" which makes the CCG responsible for complying with the GDPR and says that the CCG must be able to demonstrate compliance.

For further information relating to the accountability principle please see: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/accountability-principle/

6.7. National Data Guardian Data Security Standards

The National Data Guardian (NDG) Data Security Standards have been developed as a result of the National Data Guardian Review of Data Security, Consent and Opt-outs. These outline measures to ensure information at rest and in transit is secure. There are 10 standards which are clustered under 3 leadership obligations to address people, process and technology issues.

Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes – this standard ensures the secure transfer of information.

For more information on all the 10 Data Security Standards please refer to: https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

6.8. The Caldicott Principles

Before using or sharing confidential information, the Caldicott Principles ask that staff consider; whether they need to actually access the information, if they do how they handle the information whilst in their possession and a reminder that sharing information (principle 7) can be just as important, as long as principles 1 - 6 have been considered:

Principle 1 - Justify the purpose(s) for using confidential information
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.

Principle 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).

Principle 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.

Principle 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.

Principle 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.

Principle 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.

Principle 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

The following sections (7 – 21) provide guidance to staff on how data should be processed to reduce data being placed at risk.

7. Data Security in the Work Environment

7.1. Secure Transfer of Data procedures should be in place in any location / office environment where confidential data is being processed and transferred / transmitted especially where the data is personal data / special category data or business sensitive.

7.2. When choosing such an environment, the follow factors must be considered:

- The office or workspace must be lockable and / or accessible via a coded key pad (or similar device) and be accessible only to authorised staff;
- If the office or workspace is sited on the ground floor, windows must be lockable and screens must be located so they cannot be seen by unauthorised personnel through the windows;
- Locked doors should not be propped open;
- Escort visitors and check they are authorised;
- Computers must not be left on view so that members of the general public or staff who do not have a justified need to view the information can see personal data;
- If moving away from a computer / laptop screen it must be locked. Select CONTROL + ALT + DELETE and hit the enter key. Or select the WINDOWS KEY + L to quickly lock a screen;
- If a colleague's device has been left open and unlocked, it should be locked on their behalf and a reminder left for them not to do so in future;
- Computers or laptops must be switched off when not in use.
- Only CCG approved encrypted laptops / desktops are to be used which include encryption software
- Information must be held on the CCGs secure network and not on desktops (e.g. C: Drives).
- Passwords / passphrases must not be shared. Strong passwords must be used on all your devices to prevent unauthorised access. Different passwords should be used for each account. Creating strong passwords is not a daunting task if simple guidelines are followed. The National Cyber Security Centre (NCSC) has a range of guidance on good password management, including this article to help you set secure passwords: https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0 ;
- Manual paper records containing confidential data must be stored in locked cabinets when not in use and securely stored when the office / workstation is left unattended. Make documents are locked away if the desk is unoccupied during the day, evenings and weekends;
- Documents should not be left unattended for any significant period of time e.g. post should not be left unattended in post trays or on desks;
- Post trays should be situated away from any unauthorised access and situated where they can be monitored and mail must be disseminated to the addressee as soon as possible;
- Secure printing facility enabled on all printers used by CCG staff.

8. Transfers of Data by Email

8.1. Personal data and / or business sensitive data must always be sent via NHSMail or an NHS approved encrypted email system. NHSMail accounts have the suffix @nhs.net. (firstname.secondname@nhs.net), emails will be sent / received via the encrypted NHSMail service.

8.2. Please note NHS accounts which end in @nhs.uk **may not be secure (see section 8.7).** If you are sending personal data and / or business sensitive data and are unsure whether you are sending to an encrypted email account, always ask.

8.3. Organisations external to the NHS such as local authority / councils, local providers e.g. care homes have different email accounts. The list below states those non NHS domains where emails can be sent to and from an NHSMail account and it will be sent encrypted and therefore secure.

- *..gov.uk for local and central government
- *.cjsm.net and *.pnn.police.uk for Police/Criminal Justice
- *.mod.uk for Ministry of Defence

8.4. When emailing personal data and / or business sensitive data to outside third party organisations that do not have NHSMail, they must have either an approved email encryption software (AES) system in place and / or the NHSMail process for sending emails securely to non NHSMail accounts must be used.

8.5. NHSMail process for sending emails securely to non NHSMail accounts

8.5.1. NHSMail users can now send encrypted and secure emails to non NHSMail accounts (non-accredited or non-secure recipients) including Gmail, Hotmail etc.

8.5.2. When you enter **[secure]** in the subject line of the email and click send, the email is encrypted and protected with a digital signature on the NHSMail platform within the UK. The recipient will be asked to authenticate to the service (they will receive an alert from the Egress Web Portal and be asked to 'Open Message' where they will need to enter their password).

8.5.3. The formatting of the message will be preserved and attachments can be included. Please be aware some attachments are not supported, more information about this can be found in the NHSMail Attachments Guide – see link below. The sent item will be stored in your Sent Items folder, and any replies received will be decrypted and displayed as normal in NHSMail. The recipient will be able to reply, forward the email on and it will still remain secure and encrypted.

8.6.4. For further details please refer to the NHSMail Encryption Guide – this can be sent onto to your recipients in advance to help with the set up. You can access this on the link below:

- https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/encryptionguide.pdf

8.6.6. How to send an encrypted email from an NHSMail account:

1. Using your NHSMail account as normal, create a new message as normal
2. Ensure the recipients email address is correct
3. In the Subject field of the email, type the word **[secure]** before the subject of the message. The word secure must be surrounded by the square brackets for the

message to be encrypted. If square brackets are not used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment

4. Type your message
5. Send the email as normal

Note: [secure] is not case sensitive and [SECURE] or [Secure] for example could also be used.

8.7. NHS Digital Secure Email Standard

8.7.1. Various Organisations are looking at achieving NHS Digital Secure Email Standard (DCB1596), meaning once achieved the organisation will be able to email securely from their email accounts. Organisations looking to become accredited are required to undergo a vigorous assessment by NHS Digital and once passed they receive a Conformance statement for NHSmail.

8.7.2. This would mean you would not need to use the [secure] method (section 8.6) and the organisation could email to your NHSmail account (and vice a versa) as normal, as you do with NHSmail colleagues.

8.7.3. You will notice that these organisations who have NHS Digital Secure Email Standard will still keep their email addresses ending in co.uk, nhs.uk etc. So to keep up to date with accredited organisations refer to this link:

https://digital.nhs.uk/nhsmail/secure-email-standard - Under 'Conformance statements'

8.8. Email Awareness Tips

- Never automatically "reply all" always check all the email addresses are correct and it is appropriate that they are included in your response. If someone within the chain has made a mistake and you "reply all" you will be repeating the error and this could end in an unauthorised disclosure which could result in a CCG Data Security breach / IG Incident which may be reportable to the ICO. This could potentially result in a monetary fine and more importantly a loss of public trust.

- Always carefully check email addresses before you send an email. NHSMail is a national system which contains similar email address for the same name. E.g. there can be a Mickey.mouse1@nhs.net and a Mickeymouse1@nhs.net The only difference is a dot and it's very easy for a mistake to occur! The incorrect email can automatically pop up in future emails if you do not clear it from your contacts.

- Always ensure you regularly review any distribution lists (DL) you have to ensure all the recipients are still current and correct.

- Do you know the difference between "TO" "CC" and "BCC"? The consequences of not understanding the difference can be a data breach

    - **TO** is the person exactly to whom you are sending the email. Generally the whole purpose of the email is to express or pass information to the person who is in the TO field.

- **CC** stands for Carbon Copy. When writing emails the actual recipients address will be included in TO field of the mail application. People who are not directly involved or acting on the subject matter will be included in CC field for information purposes.

- **BCC** stands for Blind Carbon Copy, which is exactly similar to CC but the email addresses included in the BCC field will not be visible to anyone else other than the particular recipient. This function is particularly important where you wish to send an email to a distribution list without disclosing email addresses to other email recipients who do not need to know the email addresses of others.

- Emails which contain personal data should always be appropriately titled i.e. do not include confidential details in the subject line such as name.

- If you do send an email in error, you can use the recall facility 'recall this message' (please note this function is only available in Outlook and not web based NHSMail). If the recipient hasn't read the message it will be removed from their inbox. If they have opened the message a recall message will make them aware that the message was not meant for them and they may delete it, although they won't be prompted to do so and may have already read the information.

- If you have sent an email containing personal data in error you must report it immediately following the CCG's incident reporting procedures. For further information relating to incidents please follow the Data Security Breaches / Incident Reporting Procedure which is located on the CCG website.

- Tidy up your contacts list and any distribution lists regularly to ensure out of date emails addresses do not pop up automatically and to ensure any leavers / authorised recipients are not included in the distribution list.

- Never disclose passwords or log on details to anyone, even a colleague, those details are private and must remain so.

- If you receive an unsolicited email containing an attachment or a link that you have not asked for do not open it or click on it as it as you could be subject to a phishing attack. This is where criminals or hackers sometimes use a link or attachment as a way to install malicious software on your computer.

Further information relating to email can be found on the CCG Acceptable Use Policy (Including IT Email and Internet) which is located on the CCG's website.

Lastly: Always check the recipients email address is correct before you press send.

9. Telephone Disclosures

9.1. There will be occasions when telephone enquiries are received asking for disclosure of personal data. Staff are expected to apply common sense with regard to the open plan office and use an available private room for telephone conversations that are highly confidential. When the disclosure is legally justified and the caller has a legal right to access that information, the following rules should be adhered to:

- Verify personal details including the name, job title and organisation of the person requesting information;
- Obtain and record enquiries telephone number;
- If the caller is part of an organisation / company, the main switchboard number of that organisation (via phone book or directory enquiries) should be obtained and ring back;
- Conduct the call in area that is private / confidential where staff / public cannot overhear – you could be talking about a relative / neighbour of a work colleague who is listening to your conversation;
- Any notes made during the calls should be kept in a secure place (locked away) and not left on any desk;
- If in doubt, the caller should be advised that they will be called back and where necessary, a senior manager or the designated authority for confidentiality issues should be consulted if necessary;
- Any suspect bogus enquiries should be referred immediately to the IG Team or DPO as soon as possible and an incident logged;
- Always provide the minimum amount of information that is necessary;
- Provide the information only to the person who requested it and do not leave a message;
- Be aware of any press enquiries and refer to the Communications department.

10. Transfers of Data by Post

10.1. The following rules must be followed when sending / receiving personal data via post:

Incoming:

- Ensure incoming post is received in an environment away from / unauthorised public interference e.g. not left on desks or in a waiting / public area;
- Open incoming mail away from public areas;
- Ensure if post is sorted for onward distribution that it is stored securely prior to dissemination and regular deliveries are made so there is no delay in receipt of the information for the receiver and is picked up frequently.

Outgoing:

- Check if you need to use a courier / “signed for” Royal Mail service to post to ensure receipt of delivery;
- Always double check the contact details / address of the recipient or the recipient’s representative;
- Ensure the recipient’s contact details are clearly labelled on the envelope / package;
- If the envelope contains confidential data, mark the envelope clearly as ‘Private and Confidential’;

- Use a CCG letter headed front page or compliment slip;
- Use a secure robust envelope, include a return address where appropriate;
- For important letters / parcels, ask for confirmation of safe arrival.

11. Manual transfers of Paper / Hardcopy Documentation

11.1. Paper records / documents / hard copies of electronic information may be required for investigation or to refer to as part of patients care. The following rules must be followed regarding confidential paper documentation:

- Paper documents that contain confidential information must be stored in a lockable cupboard or cabinet prior to sending (if they have to be stored);
- Lockable crates must be used to move bulk hardcopy information;
- Only take off site, the minimum amount of paper documentation that is necessary;
- Record what paper documentation is taken off site / from a department (particularly if this is patient information), and if applicable, where and whom the information has gone to, perhaps keep a logbook;
- Ensure documents such as case notes are properly 'booked out' of any relevant filing system if this system is in place;
- Never leave personal / sensitive / confidential records / documents unattended – ensure they are always stored securely when not required;
- Ensure the information is returned as soon as possible and record that the information has been returned in the log. Or if you no longer need the paper documentation, ensure this is confidential disposed of using the CCG's confidential waste processes;

11.2. For further information on the security of paper documentation please refer to the CCG's Records Management Policy (located on the CCG website) and the Records Management Code of Practice for Health & Social Care 2016 on the following link:

https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

12. Transfers of Data to Photocopiers / Printers

12.1. The CCG has secure printers / photocopiers which requires you to swipe your identity card in order for you to collect your printed documents. Please ensure that when you have printed your documents particularly if these contain confidential information / personal data that you check the output tray and do not leave any documentation behind. If there is no secure printing facility available do not print unless this you are in a secure environment where unauthorised access to the printed material cannot occur.

13. Transfers of Data via Text Message

13.1. Text messaging is becoming increasingly popular between staff. The following must be considered before any text messages are used:

- Check the mobile number is correct and be confident that the person using the recipients mobile is the person to whom the message is intended;
- Keep messages short;
- Do not transfer business sensitive or personal data via text;
- Mobile phone networks may be open to additional risks of eaves dropping or interception;
- Remember data sent via text message could be released via a Freedom of Information request and / or a right of access request.

14. Transfers of Data using Portable Devices

14.1. The use of portable devices such as laptops, mobile phones, smartphones / tablets, USB memory sticks to transfer and store information for work purposes must be in line with CCG policy and authorised by your line manager (and the CCG IT Services provider, where appropriate).

- Only portable devices that are approved by the CCG and are encrypted to NHS standards (and where appropriate have up to date anti-virus software) can be used for work purposes to transfer data with and or store data.

- Personally owned portable devices such as laptops, smart phones, tablet devices must not contain work related information / information assets and must not be directly connected to the corporate network either by a direct network cable connection or Wi-Fi connection. However, such devices may be connected to the CCGs ‘guest’ Wi-Fi service but only if in accordance with the full suite of IT / Data Security / Information governance policies and procedures.

- Data on laptops must always be stored on the secure network folders. When off site, you can access this via VPN / remote access token. Never store data on the local drive of a laptop, this is insecure.

- In order to be issued with a portable device a member of staff must complete the required approval forms and have it authorised by their Line Manager.

- All security and encryption features on portable devices must be utilised such as username and password authentication. Where additional safeguards can be put in place they must be done so such as a minimum 4 digit PIN being allocated to a mobile phone.

- For any issues related to use of the portable device such as malfunction - staff members should contact IT Services.

- When staff leave the CCG they must return any equipment provided by the CCG (this may be through a designated contact point at the CCG if not directly through the IT service).

15. Transfers of Data by the NHS Secure Electronic File Transfer (SEFT) Service

15.1. Secure Electronic File Transfer (SEFT) works by providing a secure wrapper around any file, regardless of its size, structure or data content. SEFT provides data security during transmission (by using a 256-bit AES encryption mechanism). The data are held in secure containers at NHS Digital and only people who are authorised to process the data are allowed access.

15.2. SEFT can only be accessed by registered and approved users. Further information can be found on the link below:

https://digital.nhs.uk/services/transfer-data-securely

16. Transfer of Information to Cloud Storage

16.1. 'Cloud storage' is where you can upload documents, photos, videos and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet etc.). Any changes made to these files are automatically copied across and immediately accessible from other devices you may have.

16.2. For work purposes, all data must be stored securely on network folders and these can be accessed remotely via VPN when off site. However there may be occasions when you may need to use cloud storage. Always check with the CCG IT Manager and / or the IT provider to see if this can be approved and also which cloud storage providers can be used as not all are approved for use in the NHS. This is important as when data is stored in a cloud that this means they are really just stored on servers controlled by the service provider. Some providers of cloud services may also use the cloud services of another organisation. Therefore, it is essential that the security and availability of the service is right for the types of files you want to upload. For more information about cloud storage, please visit the ICO pages below:https://ico.org.uk/your-data-matters/online/cloud-computing/

17. Non Routine Bulk Transfers

17.1 Any non-routine bulk extracts (50+ records) or transfers of personal or special category data must be authorised by the responsible manager or the Information Asset Owner for the work area and may require approval by the SIRO and / or the DPO.

17. Transfers of Data via Social Media Platforms

17.1 Transfers of business confidential information / personal data to social media platforms is not permitted. Only approved information by the CCG is published on social media platforms such as Twitter and Facebook. These platforms must not be used to transfer / store business information or to discuss any work related issues.

18. Transfers of Data via Audio Recordings

18.1. The recording of audio is a useful tool to record an event, for example, to record minutes of a meeting or review in order for accurate minutes / reports to be produced from this. If any meetings are to be recorded then only approved CCG equipment must be used and those in attendance at the meeting must be informed. The recording must be deleted from the audio recording device as soon as practicable and the device must always be locked away when not in use. For further information, please visit the ICO pages below:

https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/scenarios/audio-recordings/

19. Transfers of data via photography and video equipment

19.1. Use of digital photography and video recording provide a permanent record of an event for a range of different purposes. Such devices rarely contain the ability to encrypt images stored on the device. As a result there is a risk of unauthorised access if the device, or a removable memory card, is lost or stolen.

19.2. Therefore, it is important that images / recordings from a camera / recording device are transferred to a secure location and the remaining content deleted from the memory card / device as soon as is practical.

20. Transfers of Data Overseas

20.1. If there are any occasions when you need to transfer business sensitive / personal data overseas, always seek the advice from the IG Team or DPO in the first instance. The security of the transfer and the recipient arrangements for security must be checked prior to any transfers being made.

21. Disposal / Deletion of data

21.1. All users must ensure that, where equipment is being disposed of, all data on the equipment / device is securely destroyed; this can be arranged by contacting the CCGs IT Service Provider.

21.2. Any paper documentation that is no longer required following transfer must either be filed away securely and / or securely disposed of using the confidential waste bins / containers situated across the CCG office. Please ensure that you inform the IG Team or DPO if the confidential waste bins / containers are full so these can be emptied as soon as possible. For further information regarding records management, please see the CCG's Records Management Policy and the NHS Records Management Code of Practice for Health & Social Care 2016.

21.3. When staff use portable devices to transfer / temporarily store data, for example, via USB devices, the data must be deleted as soon as no longer required.

21.4. For more detail re security please see the NHS Digital Keep it Confidential Campaign - https://keepitconfidential.nhs.uk/campaign/

22. Monitoring and Review

22.1. This policy will be reviewed every 2 years, and in accordance with the following as and when required:

- Legislative changes
- Good practice guidance
- Case law
- Significant incidents reported
- New vulnerabilities
- Changes to CCG organisations structure

23. Legislation and related documents

23.1. This procedure is available on the CCG's Intranet and Internet.

23.2. A number of other policies are related to this policy and all employees should be aware of the full range below:

- IG001 Information Governance Policy
- IG002 Confidentiality and Data Protection Policy
- IG003 Corporate Information Security Policy
- IG004 Acceptable Use Policy (IT, Email and Internet)
- IG005 Records Management Policy
- IG006 Information Risk Policy
- IG007 Data Security & Protection and Incident Reporting Procedure
- IG009 Confidentiality Audit Procedure

23.3. Acts Covered Under Policy

- General Data Protection Regulation 2016
- Data Protection Act 2018
- The National Data Guardian Data Security Standards
- Confidentiality: NHS Code of Practice
- Common Law Duty of Confidence
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000

23.4. The CCG will also take action to comply with any new legislation affecting Secure Transfer of data as it arises.

24. Links and further information

- Data Protection Act 2018
  https://www.gov.uk/government/collections/data-protection-act-2018
- General Data Protection Regulation 2016 (GDPR)
  http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- IG Alliance (IGA)
  https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga
- Records Management Code of Practice for Health & Social Care 2016
  https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016
- Information Commissioners Office (ICO)
  https://ico.org.uk/
- The NHS Care Record Guarantee
- Caldicott 2 - Information: To Share Or Not To Share? The Information Governance Review. London: Independent Information Governance Oversight Panel, 2013
- Caldicott 3 - Review of Data Security, Consent and Opt-Outs. :National Data Guardian, 2016
- Guidance on sending a secure email from an NHS Mail Account to a non NHS Mail account
  https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC_Sending%20an%20encrypted%20email%20from%20NHSmail%20to%20a%20non-secure%20email%20address.pdf
- British Medical Association – GDPR Guidance
  https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr
- Data Security and Protection Toolkit (DSPT)
  https://www.dsptoolkit.nhs.uk/
- Guidance regarding the Law Enforcement Directive
  https://ico.org.uk/for-organisations/guide-to-law-enforcement-processing-part-3-of-the-bill/
- The National Cyber Security Centre - Creating passwords
- The National Cyber Security Centre - Password Managers