Confidentiality Policy

Document History

Document Reference:	03
Document Purpose:	This policy sets out the expectations for Bromsgrove Primary Care Network employees are required to manage information in line with legislation and national guidance.
Date Approved:	September 2023
Version Number:	2.0
Status:	Approved
Next Revision Due:	September 2024
Developed by:	Umar Sabat, Data Protection Officer
Policy Sponsor:	Primary Care Network Manager
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the Bromsgrove Primary Care Network.
Associated Documents:	Data Protection Impact Assessment Policy, DSP Toolkit submission, Data Protection Policy, Privacy Policy

1. Introduction

1.1 Bromsgrove Primary Care Network (PCN) is committed to ensuring all information it holds is kept safe and confidential. This includes all information relating to patients, the organisation's financial and business records, and any staff information.

1.2 Bromsgrove PCN commits itself to working within the Data Protection Act 2018 the General Data Protection Regulations (GDPR), Caldicott Principles and adheres to the Confidentiality: NHS Codes of Practice 2003.

1.3 This policy has been reviewed to reflect the GDPR and Data Protection Act 2018 requirements.

2. Scope

2.1 This policy applies to all staff and contractors working on behalf of Bromsgrove PCN. All information held by Bromsgrove PCN be treated as confidential information and will not be shared outside of the organisation, unless it has been consented to or there is a requirement within a contract that requires us to. This includes patient information, HR records, and financial/ business records. However, there may be occasions where information may need to be shared without consent in order to protect an individual. Such occasions may be where there are safeguarding concerns.

2.2 This policy will set out the framework for which people will need to work within to ensure that information is kept safe, that there are appropriate access levels applied, and where information is needed to be shared, how this can be achieved safely and securely.

3. Definitions

3.1 Confidential Information – can be anything that relates to patients, staff, their family or friends, in whatever format it is stored. This includes any confidential corporate information.

3.2 Person- identifiable information – this is anything that contains the means to identify a person, for example, name, address, postcode, date of birth, NHS number, National Insurance Number. This can also include visual images, such as a photograph, which is sufficient to identify individuals.

3.3 Sensitive Information – certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirement as stated in legislation e.g., health information. All information should be considered sensitive e.g., name and address.

4. Roles and Responsibilities

4.1 It is the responsibility of the Board to have a strategic overview of all work and policies undertaken to ensure that it meets all legal, statutory and good practice guidance requirements.

4.2 The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient- identifiable information

4.3 The Information Governance Lead and Governance Lead are responsible for monitoring compliance with legislation, taking any actions to mitigate against breaches of confidentiality, and to act as lead investigator where required on data breaches.

4.4 All staff have a responsibility to keep confidential information safe and secure, and to not disclose information where it is not appropriate to do so. If staff are asked to disclose information, advice should be sought from the Information Governance Lead. All staff are expected to complete their Information Governance Training on an annual basis. Staff contracts of employment include a commitment to confidentiality so to are contractors expected to complete training. Any breaches of confidentiality could be regarded as gross misconduct and may result in disciplinary action.

5. Principles of Patient Confidentiality

5.1 All staff must ensure that the following principles are adhered to:

- Person- identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of
- Access to person- identifiable or confidential information must be on a need- to know basis
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required
- Recipients of disclosed information must respect that it is given to them in confidence
- If the decision is taken to disclose information, that decision must be justified and documented
- Any concerns about disclosure of information must be discussed with either your Line Manager or the Governance Lead.

5.2 Bromsgrove PCN is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

5.3 Person- identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

5.4 Access to rooms and offices where person- identifiable or confidential information is stored must be controlled; filing cabinets/ cupboards must be locked, with the key(s) kept in a secure place e.g. key safe.

5.5 All staff must clear their desks at the end of each day, particularly any person identifiable or confidential information which must be put away in lockable filing cabinets.

5.6 Unwanted printouts containing person- identifiable or confidential information must be shredded.

6. Requests for information and disclosure

6.1 If disclosure of information has been requested, which may have personal consequences for the patient or staff involved, consent must be obtained. If the person withholds consent, or is unable to give consent disclosure may only happen where:

- It can be justified in the public interest (usually where disclosure is essential to protect the patient or someone else from the risk of significant harm)
- It is required by law or by order of a court
- There is an issue of child protection. You must always act in accordance with national and local policies.

6.2 Everyone has the right to expect that their information will be held in confidence. Confidentiality is central to trust between health providers and patients. The following must be applied:

- Never give out information on patients or staff to persons who do not need to know
- All requests for identifiable information should be based on a justified need. Some requests may also need to be agreed by the Caldicott Guardian or Information Governance Lead
- The transfer of information may be agreed under an Information Sharing Protocol or Agreement.

6.3 If it is uncertain whether the information can be disclosed, seek advice from your Line Manager or from the Information Governance or Governance Lead.

7. Sharing Information

7.1 Use of Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/ data should be addressed to a person, a post holder, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

Where possible, window envelopes should always be used. Care should be taken to ensure only the recipient and address is displayed in the window. If it is not possible to use a window envelope, for example where the recipient has been copied into the letter, specific attention must be paid to ensure that the envelope is correctly addressed and only the intended letter inserted.

The envelope must be labelled above the addressee details, with “Private and confidential". Electronic media should always be protected. No electronic media, such as CDs, should be sent unencrypted. Advice on how to protect files is available from the Information Governance Lead.

7.2 Emailing Confidential Information

Special care should be taken to ensure the information is sent only to recipients who have a “need to know “. You must always double check you are sending the mail to the correct person/s. All staff have a personal responsibility to ensure that all personal or sensitive information is sent and received in a secure and confidential manner. It is the sender’s responsibility to ensure that all the information being sent is accurate and that the recipient’s details are correct. Any incidents regarding a breach of this should be reported immediately as an incident via the incident reporting system.

You must include the phrase” Patient Information" in the subject field; this ensures that the message is clearly identifiable to the authorised addressee. If you are sending an email containing sensitive information outside of Bromsgrove PCN you must first establish if it is legal to do so. Sharing information without consent could be a breach of the Data Protection Act 2018 GDPR. If in doubt, please contact the Information Governance Lead for advice.

Person identifiers should be removed wherever possible, and only the minimum necessary information sent, this may be considered to be the NHS number but no name or address. This in itself can pose problems as the wrong number may be typed.

External transfers should only take place to persons with access to a secure email address. Under no circumstances whatsoever should any type of patient identifiable information, sensitive or confidential information about any person be emailed to persons who only have

private email addresses, such as hotmail.com or gmail.com accounts without the permission of the Information Governance Lead. Due to its insecure nature any information transmitted over the Internet should be considered to be in the public domain.

8. Working Remotely

8.1 There may be occasions where Bromsgrove PCN staff will need to work remotely. This includes staff who are working from home, working outside of Leicestershire or are working from another location delivering services where access to the Bromsgrove PCN domain is required. In these circumstances:

- Staff can only use equipment that has been provided by Bromsgrove PCN due to the security and encryption already set up on these devices
- Staff are not to email any of their work to their personal email addresses to work on from home, or save any work on their personal computers.
- There may be occasions when patient information is taken home. If this is required, this should be discussed with your Line Manager or the Information Governance Lead whether this is appropriate. If it is deemed appropriate, no patient information is to be left in the staff member's car but to be taken into the staff member's home. All passwords are to be kept confidential and not to be shared with wider members of the organisation.

9. Carelessness

9.1 All staff have a legal duty of confidentiality to keep person- identifiable or confidential information private and not to divulge information accidentally.

9.2 Staff may be held personally liable for a breach of confidence. The following steps will help staff to keep personal and confidential information safe:

- Do not talk about patients or the organisation's business in public places or in places where you may be overheard
- Do not talk about patients or the organisation's business in social media environments • Do not leave any confidential information out unattended
- Ensure that the public cannot see computer screens, or other displays of information
- When leaving your desk, ensure that the computer is locked (Ctrl + Alt + Delete, or Windows key + L) • Any portable forms of data must be locked in a drawer/ filing cabinet
- Do not disclose your passwords to anyone

10. Abuse of privilege

10.1 It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 2018 and GDPR.

10.2 When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of Bromsgrove PCN.

10.3 If staff have concerns about this issue, they should discuss it with their Line Manager or Information Governance Lead

11. Equality Impact Assessment

11.1 An initial Equality Impact Assessment has been carried out on this policy, and it has been deemed that there are no positive or negative impacts on any of the protected characteristics. Therefore, a full Equality Impact Assessment is not required.