Data Protection Policy

1. Implementation & Review

Implementation Date:	July 2018
Review Cycle:	Every 2 years
Last Review Date:	January 2024
Next Review Date:	January 2026

2. Introduction

The Humberside Group of Local Medical Committees Ltd ('the company') needs to gather and use certain information about individuals.

This can include information about our GP constituents, staff (e.g. Practice Managers) at our local practices and LMC members and observers. It can also include information about our suppliers, business contacts, employees, prospective employees, company directors and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

3. Why this policy exists

This data protection policy ensures that The Humberside Group of Local Medical Committees Ltd:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, constituents, members and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

4. Data Protection Law

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) describe how organisations must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by seven important principles. These are that personal data must:

1. Be processed fairly, lawfully and transparently.
2. Be obtained only for specific, lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Be processed in a manner which maintains the security, integrity and confidentiality of the data, and;
7. That we are accountable for, and can demonstrate compliance with, the above data protection principles

5. Scope of Policy

This policy applies to:

- The head office of The Humberside Group of Local Medical Committees Ltd.
- Any branches of The Humberside Group of Local Medical Committees Ltd that may be opened at any time in the future.
- All staff and Directors of the company.
- All contractors, suppliers and other people working on behalf of the company.

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ….. and any other information relating to individuals

6. Data protection risks

This policy helps to protect the company from some very real data security risks including:

- **Breaches of confidentiality** e.g. information being given out inappropriately.
- **Failing to offer choice** e.g. not seeking informed consent where this is the established legal basis for processing certain types of data.
- **Reputational damage** e.g. the company could suffer if hackers successfully gained access to sensitive data.

7. Responsibilities

Everyone who works for or with the Company has responsibility for ensuring that data is collected, stored and handled appropriately.

Each individual that handles personal data on behalf of the company must ensure that it is handled and processed in line with this policy and data protection principles. In addition, these people have key areas of responsibility:

The Board of Management is ultimately responsible for ensuring that the company meets its legal obligations.

The Senior Management Team is responsible for operational oversight of the day to day implementation of this policy and for:

- Keeping the Board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies in line with the agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the Company holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Ensuring that IT services provided to the Company include regular checks and scans to ensure security hardware and software is functioning properly. (Service currently provided by N3i Foundation Trust.)
- Evaluating any third-party services the company is considering using to store or process data e.g. cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with other staff to ensure that marketing activities abide by data protection principles.
- Following the correct procedure in the event of a data breach

8. Guidelines for all staff members

The following guidelines must be implemented by all employees of the company:

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **must not be accessed or shared without good reason**. When access to confidential information is required, employees can request it from their line managers.
- The company will **provide training** to all employees to help them understand their responsibilities when handling data.

- **Sensible and common-sense precautions** should be taken to ensure that all data is kept secure, and care should be taken to ensure that is accurate and kept up to date (in particular, through the use of our Customer Relationship Management systems (CRM)). Where privacy-protecting technology or other measures are made available by the company, it must be used (for instance, using specialist mailing and event-management tools rather than BCC-ing bulk emails).
- **Strong passwords** must be used and must never be shared.
- Personal data **must not be disclosed** to unauthorised people, either within the company or externally.
- Data must be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be **deleted and disposed of securely**.
- **Physical security measures** should be implemented at all times. This includes ensuring that confidential filing cabinets are kept locked, that doors are locked and alarms are set when the office and/or building is unoccupied and that access to the building is appropriately managed.
- Employees should **request help** from their line manager or a member of the Senior Management Team if they are unsure about any aspect of data protection or suspect a data breach.

9. Data Storage

This section of the policy describes how and where data should be safely stored. Questions about data storage can be directed to the CEO MD or, in their absence, another member of the Senior Management Team.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Employees should make sure that printouts are **not left where unauthorised people could see them**, such as on a printer or in open view in a publicly accessible office.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically,** it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords that are changed regularly** and **never shared between employees**.
- If data is stored on removable media (like a CD or DVD), these should be **kept securely locked away** when not being used. Encrypted media should be used where possible.
- Data should **only be stored on designated drives and servers**, and should **only be uploaded to cloud computing services that have been approved by the Company for such use**.
- Data should **never be saved directly to laptops or other mobile devices** like tablets or smartphones, as it will not be possible to recover it if the data is lost.

The company will be responsible for ensuring that:

- Servers containing personal data are **sited in a secure location**, with appropriate security measures in place.
- Data is **backed up frequently**.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

10. Data Use

Personal data is of no value to the Company unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. To ensure safe usage of data, the following guidelines will be followed:

- When working with personal data, employees should ensure the **screens of their computers are always locked** when left unattended.
- Any **sensitive personal data which has not been anonymised should only be sent from and to a registered NHSmail address**. This is the secure email service approved by the Department of Health for sharing patient identifiable and sensitive information meaning it meets a set of information security controls that offer an appropriate level of protection against loss or inappropriate access. Sensitive personal data should never be sent either from or to an email address that is outside of the NHS mail service unless it is properly encrypted. The Business Support Officer can explain how to **encrypt data to send to authorised external contacts who do not have access to NHSmail**.
- Personal data should **not be transferred outside of the European Economic Area** unless it is being processed by an organisation which can demonstrate that it has in place an adequate level of protection, for example, the EU-US Privacy Shield certification. If employees intend to transfer data outside the European Economic Area, please discuss this with a member of the Senior Management Team first.
- Employees should **not save copies of personal data to their own computers**. Always access and update the central copy of any data.

11. Data Accuracy

The law requires the Company to take reasonable steps to ensure that data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort the Company should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible including:

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should take **every opportunity to ensure data is updated**. For instance, by confirming the details of a GP or Practice Manager when they call.

- The company will make it **easy for data subjects to update the information** the company holds about them.
- Data should be **updated as soon as inaccuracies are discovered**. For instance, if a GP can no longer be reached on their stored telephone number, it should be removed immediately from the database.

12. Data Breaches

A data breach means a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are both accidental and deliberate. It is important to note that a data breach is more than just losing personal data.

Examples of data breaches include where any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Humberside LMCs would like to encourage a transparent reporting culture, so that information security arrangements can be reviewed and refined. If a member of staff suspects that a data breach has occurred, or has experienced a near miss, this also needs to be reported.

If a staff member becomes aware of a data breach, this breach needs to be reported immediately to the CEO MD. The following information should be provided where possible / appropriate:

- Description of the data breach.
- When the breach occurred / when the LMC became aware of the breach.
- The type of personal data involved.
- Approximately how many people have been affected.
- Whether any children are involved.
- The employees involved.
- Any immediate steps taken to rectify / mitigate the data breach.

The CEO MD will then discuss the matter with the staff member to determine the next steps, and whether a notification needs to be made to the ICO, and/or any other bodies (for example, the police, or other professional bodies). Consideration will also be given to appropriate internal employees to inform (for example, line managers).

A record should be made of all data breaches (even if it is not reported to the ICO). If the matter is not reported to the ICO, a record should be made of the reasons for this. As a minimum, this record should include the facts relating to the breach, its effects and the remedial action taken.

Guidelines for Handling a Data Breach:

- *Data breach involving shared data where the LMC is acting as a Data Controller:*

Where the LMC is acting as a data controller and becomes aware of a data breach by a data processor, it will be responsible for leading the investigation and determining the response to the breach. This will include corresponding with the ICO, notifying affected individuals and any third parties, as well as leading on any remedial action.

Any affected individuals should be notified without undue delay if the risk from the incident is likely to result in a high risk to an individual's rights and freedoms. The following information will need to be provided:

1. The name and contact details of a contact point where more information can be obtained.
2. A description of the likely consequences of the personal data breach.
3. A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Consideration will also be given to whether to notify other employees (such as HR) or other agencies (for example the police).

- *Reporting to the ICO by the LMC:*

Not all data breaches need to be reported to the ICO, but where this is necessary the ICO should be notified within 72 hours of the LMC becoming aware of the data breach, even if all the details are not yet available. Information should then be provided to the ICO in phases if necessary. The ICO should be informed if this is the approach which will be used.

The matter should be reported to the ICO unless it is unlikely there will be a risk to people's rights and freedoms. An incident is more likely to be reportable if the data breach is severe, concerns sensitive personal data, malicious intent, or a large number of people. Each data breach will need to be considered on a case by case basis. For example, data breaches which could result in a risk of discrimination, identity theft or fraud, financial loss, damage to reputation, and loss of confidentiality are likely to be considered severe and reportable to the ICO on the basis they prejudice individuals' rights and freedoms.

If the LMC is not sure whether to report a breach to the ICO, use the ICO's self-assessment tool, located here: https://ico.org.uk/for-organisations/report-a-breach/pdb-assessment/. It may be appropriate to seek legal or professional advice on reporting.

If the matter is to be reported to the ICO, the following information should be provided:

1. A description of the nature of the personal data breach including, where possible:
    a. the categories and approximate number of individuals concerned and
    b. the categories and approximate number of personal data records concerned.
2. The name and contact details of the data protection officer or other contact point where more information can be obtained.
3. A description of the likely consequences of the personal data breach.
4. A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If a breach needs to be reported to the ICO, please use the ICO's precedent reporting form located here: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ or report by phone.

- *Data breach involving shared data where the LMC is acting as a Data Processor:*

Where the LMC is acting as data processor (i.e. it is handling data on behalf of another organisation) and becomes aware of a data breach, it must notify the relevant data controller as soon as it becomes aware without undue delay and set out the information as follows:

- Description of the data breach
- When the breach occurred / when the LMC became aware of the breach
- The type of personal data involved.
- Approximately how many people have been affected.
- Whether any children are involved.
- The employees involved.
- Any immediate steps taken to rectify / mitigate the data breach.

The data controller will be responsible for leading on the investigation and notifying the ICO.

The LMC must act in accordance with the relevant data processing agreement in place for the data sharing scenario. This will include as a minimum providing all reasonable information and support to the data controller in the management of the data breach.

If the LMC is acting as a data processor, it will not ordinarily communicate with the ICO or affected parties directly (unless required to do so by the data controller) and should send any such correspondence relating to the data breach to the data controller.

13. Subject Access Requests

All individuals who are the subject of personal data held by The Humberside Group of Local Medical Committees Ltd are entitled to:

- Confirmation that the company is processing their personal data.
- A copy of their personal data.
- Other supplementary information, the majority of which is outlined within the company's privacy notices.

If an individual contacts the company requesting a copy of their personal data, this is called a Subject Access Request (SAR).

Training will be provided to all staff in how to recognise and respond to a Subject Access Request.

An individual can make a subject access request to the Company either verbally or in writing and to any part of our organisation, including by social media.

Please refer to Appendices One and Two for full details regarding the Procedure for Responding to a Subject Access Request.

Individuals may have other rights under data protection law, or the ability to complain about how we have used their information. Complaints or other requests to access data should be referred to the CEO MD.

14. Disclosing Data for Other Reasons

In certain circumstances, the law allows personal data to be disclosed to third parties (including law enforcement agencies) without the consent of the data subject.

Under these circumstances, the Company may disclose requested data. However, the Company will ensure the request is legitimate and the disclosure is lawful, seeking assistance from the Board and from the company's legal advisors where necessary.

15. Providing Information

The Humberside Group of Local Medical Committees Ltd aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used.
- How to exercise their rights.

The company has therefore produced privacy notices, setting out how data relating to individuals is used by the company.

A copy of these Privacy Notices can be made available to any individual requesting one and they are also available on the Company's website.