Friends Medical Service

Information Security Policy

Non-Controlled Document if Saved/Printed

Review period	Annually
Approved by	Managing Director via isoTracker
Distribution	Electronic copy to FMS Staff

Document Version Control

Version	Date	Author	Comment/Summary of Changes
0.1	07/08/2020	IG Consultant	Draft
0.2		Uzair Baloch	Review and approval by IGC
1.0	05/07/2021		Approved by the Board
2.0	07/12/2021	Zaheer Baloch	Minor text changes throughout
2.1	07/05/2023	Uzair Baloch	Additional info on Pabau added
2.2	See header	Milo Burns	The Access to Health Records (Northern Ireland) Order 1993 added

Non-Controlled Document if Saved/Printed

Contents

Non-Controlled Document if Saved/Printed

Non-Controlled Document if Saved/Printed

1 INTRODUCTION

1.1 This top-level information security policy is a key component of the Friends Medical Service (FMS) overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

1.2 This policy outlines the legal, regulatory and best practice framework that this Organisation works to and the methods we will use to deliver and maintain this policy.

1.3 This document defines the information security principles and objectives for FMS. It outlines the systems that ensure current information security obligations are met and how changes, performance and incidents are governed. This document sets the policy, stating the required standard.

1.4 Information is an asset that, like other important business assets, is essential to our organisation's business and needs to be suitably protected. Its security must be maintained to the standards expected in law, regulations and contract.

2 OBJECTIVES OF THIS POLICY

2.1 The objectives of FMS' Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2 The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by FMS by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day-to-day business.
- Protecting information assets under the control of the organisation.

3 SCOPE OF THE POLICY

3.1 This policy applies to all records, information and data held and processed by FMS.

Non-Controlled Document if Saved/Printed

4 LEGISLATION

4.1 FMS is obliged to abide by all relevant UK and European Union legislation.

4.2 The requirement to comply with this legislation shall be devolved to employees and agents of FMS, who may be held personally accountable for any breaches of information security for which they may be held responsible.

4.3 FMS shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Access to Health Records (Northern Ireland) Order 1993
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2001

5 KEY PRINCIPLES

5.1 All IT Systems are to be protected against unauthorised access.

5.2 All IT Systems are to be used only in compliance with relevant Company Policies.

5.3 All employees of the Company and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors (collectively, "Users"), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

5.4 All line managers must ensure that all Users under their control and direction must always adhere to and comply with this Policy as required under paragraph 5.3.

5.5 All data stored on IT Systems are to be managed securely in compliance with all relevant parts of EU Regulation 2016/679 General Data Protection Regulation ("GDPR") and all other laws governing data protection whether now or in the future in force.

5.6 All data stored on IT Systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data, and confidential information). All data so classified must be handled appropriately in accordance with its classification.

5.7 All data stored on IT Systems shall be available only to those Users with a legitimate need for access.

5.8 All data stored on IT Systems shall be protected against unauthorised access and/or processing.

5.9 All data stored on IT Systems shall be protected against loss and/or corruption.

Non-Controlled Document if Saved/Printed

5.10 The Service Manager is responsible for ensuring installation, maintenance, servicing, repair, and upgrade of IT systems under the direction of the Managing Director.

5.11 The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with the Board unless expressly stated otherwise.

5.12 All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the Board (the Managing Director is also the Data Protection Officer).

5.13 All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the Service Manager or Managing Director.

6 MANAGEMENT OF SECURITY

6.1 Ultimate responsibility for Information Security shall reside with the Managing Director (MD).

6.2 The MD shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

6.3 The Service Manager, under the direction of the MD, shall be responsible for the following:

- ensuring that all IT Systems are assessed and compliant with the Company's security requirements;
- ensuring that IT security standards within the Company are effectively implemented and regularly reviewed, working in consultation with the MD;
- ensuring that all Users are kept aware of the requirements of this Policy and of all related legislation, regulations, and other relevant rules whether now or in the future enforce including, but not limited to, the GDPR and the Computer Misuse Act 1990.
- assisting all Users in understanding and complying with this Policy;
- providing all Users with appropriate support and training in IT security matters and use of IT Systems;
- ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities, and any special security requirements;
- receiving and handling all reports relating to IT security matters and taking appropriate action in response;
- taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;
- assisting the IT Manager in monitoring all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future; and
- ensuring that regular backups are taken of all data stored within the IT Systems. The Microsoft Teams Drive to which Board members and the Service Manager have access, is backed-up monthly onto an external drive. All data on the external drive is encrypted and the drive is kept in a securely locked cabinet when not in use. The Quickbooks system, to which the MD and Finance Manager have access, is

Non-Controlled Document if Saved/Printed

automatically backed-up into the cloud. No data accessed via Sectra is stored on FMS systems or devices.

7 DATA STORAGE SECURITY

7.1 All data, and in particular personal data, should be stored securely using passwords.

7.2 All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

7.3 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise.

7.4 No data, and in particular personal data, should be transferred to any computer or device personally belonging to a User unless the User in question is a contractor or sub-contractor working on behalf of the Company and that User has agreed to comply fully with the Company's Data Protection Policy and the GDPR.

8 DATA PROTECTION

8.1 All personal data (as defined in the GDPR) collected, held, and processed by the Company will be collected, held, and processed strictly in accordance with the principles of the GDPR, the provisions of the GDPR and the Company's Data Protection Policy.

8.2 All Users handling data for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's Data Protection Policy at all times. In particular, the following shall apply:

8.3 All emails containing personal data must be marked "confidential";

8.4 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted under any circumstances;

8.5 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

8.6 Personal data contained in the body of an email, whether sent or received, should be copied directly from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.

8.7 All personal data to be transferred physically, including that on removable electronic media, shall be transferred in a suitable container marked "confidential".

8.8 Where any confidential or personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the User must lock the computer and screen before leaving it.

8.9 Any questions relating to data protection should be referred to Zaheer Baloch, MD/Data Protection Officer, zaheer@friendsmedicalservice.com.

9 INFORMATION SECURITY AWARENESS TRAINING

9.1 Information security awareness training will be included in the staff induction process, as detailed in the Information Security Training Policy (ISTP).

Non-Controlled Document if Saved/Printed

9.2 An ongoing awareness programme shall be established and maintained, as detailed in the ISTP, to ensure that staff awareness is refreshed and updated as necessary.

9.3 New employees, contractors or third-party users will be required to attend initial information security training at in.

9.4 On a periodic basis, and at least annually, FMS shall provide refresher information security training which is mandatory for all personnel, as detailed in the ISTP.

9.5 As the organisation grows, FMS will provide detailed training to those individuals who have specific roles and responsibilities in delivering the FMS ISMS, as detailed in the ISTP.

10 CONTRACTS OF EMPLOYMENT

10.1 Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain confidentiality clauses.

10.2 Information security expectations of staff shall be included within appropriate job definitions.

11 SECURITY CONTROL OF ASSETS

11.1 Each FMS IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

12 ACCESS CONTROLS

12.1 Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

13 USER ACCESS CONTROLS

13.1 Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

14 COMPUTER ACCESS CONTROL

14.1 Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

15 APPLICATION ACCESS CONTROL

15.1 Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

16 EQUIPMENT SECURITY

16.1 To minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

Non-Controlled Document if Saved/Printed

17 COMPUTER AND NETWORK PROCEDURES

17.1 Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Board.

17.2 The Operations Director will be responsible for ensuring that software used within FMS is kept up to date and for ensuring that the latest security protections, updates and patches are installed. Wherever possible, this process will be automated. FMS uses three key software platforms to manage its business and to deliver its services. The updating and patching arrangements for each are as follows:

17.2.1 The Sectra system (as part of the Northern Ireland Picture Archiving and Communication System or NIPACS) is used for arranging patient appointments and for accessing patient details, medical records and images and entering reports. The system is cloud based and is hosted by Sectra. FMS has a contract with Sectra under which Sectra is responsible for all software updates.

17.2.2 The Microsoft 365 platform is cloud based. FMS enforces the default setting across all computers which ensures updates and patches are automatically downloaded from the internet as soon as they are available and are applied in the background.

17.2.3 The Xero financial platform is cloud based and is provided by Intuit. All software upgrades and patches are managed by Intuit.

17.2.4 Pabau is a cloud based patient information management system. FMS has a contract with Pabau under which they are responsible for all software updates.

18 INFORMATION RISK ASSESSMENT

18.1 FMS will have processes and procedures for identifying and managing information risks.

18.2 Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the corporate risk register and action plans shall be put in place to effectively manage those risks.

18.3 The corporate risk register and all associated actions shall be reviewed by Board every month. Individual risks will be managed in Risk Review meetings as required.

18.4 Any implemented information security arrangements shall also be a regularly reviewed feature of FMS risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

19 INFORMATION SECURITY INCIDENTS AND WEAKNESSES

19.1 It is the Board's responsibility to agree appropriate processes and tools to detect information security incidents, including cyber security incidents. It is the Service Manager's responsibility to ensure these processes and tools are implemented and maintained or actioned appropriately. These will include installation, maintenance and use of up-to-date antivirus software on all FMS computers, briefing staff on specific phishing approaches or trends and monitoring system logs to detect unusual or suspicious activity e.g. multiple unsuccessful login attempts against User IDs or anomalies in inbound or outbound network traffic or excessive service memory consumption.

19.2 Any information security incidents or weaknesses identified or suspected by any staff member will be reported to the MD.

Non-Controlled Document if Saved/Printed

19.3 All information security events will be investigated to establish their cause and impacts with a view to avoiding similar events in future.

19.4 Upon notification of an actual/suspected incident, the MD shall, within 1 working day, ensure the issue is assessed, including identifying the associated level of risk and shall take any and all such steps as the Board deems necessary to respond to the issue including activating the Company's Business Continuity Plan.

19.5 Under no circumstances should a User attempt to resolve an IT security breach on their own without first consulting the MD. Users may only attempt to resolve IT security breaches under the instruction of, and with the express permission of, the MD.

19.6 All IT security incidents shall be fully documented.

20 INFORMATION CLASSIFICATION

20.1 FMS will implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the NHS DSP Toolkit to secure NHS information assets.

20.2 The classification **NHS Confidential** – will be used for patients' clinical records, patient identifiable clinical information. To safeguard confidentiality, the term "NHS Confidential" shall **not** be used on correspondence to a patient in accordance with the Confidentiality: NHS Code of Practice. Note, FMS currently does not hold any patient personal data and has no plans to do so.

20.2.1 Documents marked NHS Confidential will always be held securely in a locked room to which only authorised persons have access. They will not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed packaging or locked containers. Documents marked NHS Confidential not in a safe store or in transport should be kept out of sight of visitors or others not authorised to view them.

20.3 The classification **NHS Restricted -** will be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which 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;

Non-Controlled Document if Saved/Printed

- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

20.4 NHS Restricted documents should also be stored in lockable cabinets.

21 PROTECTION FROM MALICIOUS SOFTWARE

21.1 The organisation will use software countermeasures and management procedures to protect itself against the treat of malicious software.

21.2 All staff will be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the Service Manager or MD. Users breaching this requirement may be subject to disciplinary action.

21.3 IT Systems (including all computers and servers) will be protected with suitable anti-virus, firewall, and other suitable internet security software. All such software will be kept up to date with the latest software updates and definitions.

21.4 All IT Systems protected by anti-virus software will be subject to a full system scan at least monthly.

21.5 All physical media (e.g. USB memory sticks or disks of any kind) used by Users for transferring files must be virus-scanned before any files may be transferred.

21.6 Users shall be permitted to transfer files using cloud storage systems only with the approval of the Service Manager or MD. All files downloaded from any cloud storage system must be scanned for viruses during the download process.

21.7 Any files being sent to third parties outside the Company, whether by email, on physical media, or by other means (e.g. shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate.

21.8 Where any virus is detected by a User this must be reported immediately to the Service Manager or MD (this rule shall apply even where the anti-virus software automatically fixes the problem). The Service Manager or MD shall promptly take any and all necessary action to respond to the problem. In limited circumstances this may involve the temporary removal of the affected computer or device.

21.9 Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company's disciplinary procedures.

22 MEDIA & HARDWARE SECURITY MEASURES

22.1 Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the Service Manager or MD before they may be used on FMS systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

22.2 Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised access to such locations for any reason.

Non-Controlled Document if Saved/Printed

22.3 All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by authorised individuals.

22.4 All non-mobile devices (including, but not limited to, desktop computers, workstations, and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.

22.5 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended, they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location. If any such mobile device is to be left in a vehicle it must be stored out of sight and, where possible, in a locked compartment.

22.6 The Service Manager shall maintain a complete asset register of all IT Systems. All IT Systems shall be labelled, and the corresponding data shall be kept on the asset register.

23 MONITORING SYSTEM ACCESS AND USE

23.1 Access privileges for all IT Systems shall be determined based on Users' levels of authority within the Company and the requirements of their job roles. Users shall not be granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.

23.2 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system approved by the MD. Not all forms of biometric log-in are considered secure. Only those methods approved by the MD may be used.

23.3 An audit trail of system access and data use by staff will be maintained and reviewed on a regular basis.

23.4 FMS will put in place routines to regularly audit compliance with this and other policies.

23.5 In addition, the organisation reserves the right to monitor activity where it suspects that there has been a breach of policy.

23.6 The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures

Non-Controlled Document if Saved/Printed

- Ensuring the effective operation of the system.

23.7 Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

24 Accreditation of Information Systems

24.1 FMS will ensure that all new information systems, applications and networks include a security plan and are approved by the MD before they commence operation.

25 System Change Control

25.1 Changes to information systems, applications or networks shall be reviewed and approved by the Service Manager or MD.

25.2 All changes to information systems must be subject to a privacy impact assessment to ensure any risks to confidentiality of personal and confidential data are minimised.

26 Intellectual Property Rights

26.1 The organisation shall ensure that all information products are properly licensed and approved.

26.2 Users shall not install software on the organisation's property without permission from the Service Manager or MD. Users breaching this requirement may be subject to disciplinary action.

27 Business Continuity and Disaster Recovery Plans

27.1 The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are maintained for all mission critical information, applications, systems and networks.

28 Responsibilities for Information Security

28.1 The ultimate responsibility for information security rests with the MD, but on a day-to-day basis the Service Manager shall be responsible for managing and implementing the policy and related procedures.

28.2 Team leaders are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

28.3 **All staff** shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

28.4 The Information Security Policy shall be maintained, reviewed and updated by the Service Manager or MD. This review shall take annually or when there is significant change that impacts the operation of FMS information systems.

28.5 **Line managers** shall be individually responsible for the security of their physical environments where information is processed or stored.

Non-Controlled Document if Saved/Printed

28.6 **Each member of staff** shall be responsible for the operational security of the information systems they use.

28.7 **Each system user** shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

28.8 Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

29 REPORTING

29.1 The MD shall keep the FMS Board informed of the information security status of the organisation by means of regular reports and presentations.

30 POLICY IMPLEMENTATION PLAN

30.1 Senior Management within FMS will be responsible for monitoring and implementing this policy.

30.2 Staff guidance, protocols and procedures will be developed and made accessible to staff as part of the implementation of this information security policy.

30.3 Information risk assessment will be regularly carried out to ensure that the policy is effectively implemented.

30.4 As part of implementing this policy within FMS further policies, procedures/protocols will be put in place to complement this overarching information security policy. These will cover the following;

- Access Control and Password Management
- Remote working
- Acceptable Use of FMS information systems
- Data Encryption
- Incident Management.

31 AUDIT AND MONITORING COMPLIANCE WITH THIS POLICY

31.1 FMS will undertake or commission annual assessments and audits of its compliance with legal requirements for information security arrangements.

31.2 This policy and the associated controls will be monitored through the Information Risk Management system and processes for the organisation.

31.3 Information Risk Management will be a key component of wider assurance and control in setting the priorities for FMS' information security agenda.

32 REVIEW OF THIS POLICY

32.1 This policy will be reviewed at least every two years, or as required.

Non-Controlled Document if Saved/Printed

Non-Controlled Document if Saved/Printed