Information Security Policy

Review Date 28th November 2019
Next Review Due 28th November 2021

Physiotherapy2fit Ltd is committed to ensuring that, as far as it is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on the basis of their age, disability, gender, race, religion/belief or sexual orientation. Should a member of staff or any other person require access to this policy in another language or format (such as Braille or large print) we will do our best to provide this in a format the user is able to access. Physiotherapy2fit Ltd will do its utmost to support and develop equitable access to all policies. The Director is responsible for ensuring staff are aware of Physiotherapy2fit Ltd policies and that staff adhere to them. It is also the Director's responsibility to keep staff up to date with new policy changes.

Staff are responsible for ensuring they are familiar with policies, know where to locate the documents on Physiotherapy2fit's main website, and seek out every opportunity to keep up to date with them

Independent contractors are expected to identify a lead person to be responsible for ensuring staff employed within their place of work are aware of Physiotherapy2fit Ltd policies.

Foreword

Information security is characterised here as the preservation of:

- Confidentiality (ensuring that information is accessible only to those authorised to have access);
- Integrity (safeguarding the accuracy and completeness of information and processing methods;
- Availability (ensuring that authorised users have access to information and associated assets when required).

Introduction

Physiotherapy2fit has a legal obligation to ensure that appropriate security management arrangements are in place for the protection of patient records and key information services, to meet the statutory requirements set out within the Data Protection Act 1998 and to satisfy the obligations under the Civil Contingencies Act 2004.

Physiotherapy2fit is required to demonstrate positive progress in enabling all staff to conform to the NHS Code of Practice on Information Security Management, identifying resource requirements and any related areas where organisational or system improvements are required.

The information systems, equipment, software and data used by Physiotherapy2fit represent a

considerable investment and are valuable assets, essential to the effective and continuing operation of the Physiotherapy2fit.

Much of the data held in these systems is of a confidential nature, and it is necessary for all information systems to be protected against any events, accidental or malicious, which may put at risk the activities of Physiotherapy2fit or their investment in information.

This policy applies to all Physiotherapy2fit information systems. 'Information systems' include both computer-based systems and non-computer based systems. All staff, contractors, temporary staff and third parties are required to adhere to this policy.

This policy is part of a suite of policies on information governance, available from Physiotherapy2fit's website.

Policy Statement

- The purpose of this policy is:
- To bring to the attention of all staff the need to improve and maintain security of information systems, and to advise managers of the approach being adopted to achieve the appropriate level of security.
- To ensure that Physiotherapy2fit complies with current legislation and EU Directives, meets statutory obligations and observes standards of good practice.
- To minimise the risk of security breach and prosecution.
- To meet the requirements for connection to the NHS network.

Policy

Physiotherapy2fit is committed to maintaining and developing an information systems infrastructure which has an appropriate level of security and data protection. All systems will have a minimum security framework.

In the case of local or standalone systems it is the responsibility of the Director to ensure compliance with this policy.

Sharing of information with other organisations is subject to the Protocol for Information Sharing between Health and Social Care Agencies 2006, and UK and EU Data Protection and Human Rights legislation. Where staff are unsure about sharing information they should refer to the Confidentiality Policy, or take advice from the Director.

The purpose of information systems security is to ensure an appropriate level of: -
Confidentiality: Information is obtained, held and disclosed lawfully and data access is confined to those with specified authority to view and/or change the data.

Integrity: All system assets are operating according to specification and the accuracy of data is maintained.

Availability: Systems and data are available when required and the output from it delivered to the user who needs it, when it is needed.

Passwords and Access Control

Access to electronic information systems is controlled on the basis of service requirements and managed through the use of protocols for allocating and controlling access, secure logins and passwords. Each individual is responsible for keeping their own password secure and must ensure it is neither disclosed to, nor used by, anyone else under any circumstances. Staff must only access systems using their own login and password. All staff are accountable for any activity carried out under their login and password and this is audited. **Failure to comply with these protocols may lead to disciplinary action.**

Management and Staffing Arrangements Lead responsibility for information security management rests with the Director.

Physiotherapy2fit has designated the Director as the Caldicott Guardian. She is responsible for implementing, monitoring, documenting and communicating information security policies throughout Physiotherapy2fit.

Information security should be addressed at recruitment stage for all staff, and all contracts of employment and job descriptions include a confidentiality clause

Training and Awareness

All staff will be made aware of their responsibilities for information security at the commencement of employment through the corporate induction processes. Managers will ensure that all staff they are responsible for are aware of and adhere to this policy.

Physiotherapy2fit will ensure that information security training requirements for all staff, including information governance specialists, are regularly assessed and refreshed. Training will be provided or commissioned to ensure that staff, whether clinical or administrative, are fully aware of their personal responsibilities in respect of information security and are competent to carry out their designated duties. This should include training for staff in the use and protection of both paper and electronic records systems.

Information Security Incidents

Physiotherapy2fit has adopted an electronic incident reporting system which should be used for the reporting of all incidents. The reporting, investigating and recording of any information security incidents should be in line with Physiotherapy2fit Policy for the Reporting and Management of Adverse Events and Near Misses. Serious incidents should be raised immediately with the Director.

Risk Analysis

Effective information security management is based upon the core principle of risk assessment and management. In order to make the best use of resources, each Information system should be secured to a level appropriate to the measure of risk associated with it. A risk assessment is performed, and measures will be put in place to ensure each system is secured to an appropriate

level.

Once identified, information security risks must be managed on a formal basis. Risks will be recorded within Physiotherapy2fit's risk register and action plans put in place to demonstrate effective management of the risks.

Network Connection

All network management controls and procedures will conform to the NHS wide Network Security Policy code of connection and associated guidance. This is available from the NHS Connecting for Health website http://www.connectingforhealth.nhs.uk/

Network Management is the responsibility of the Director; all devices connected to Physiotherapy2fit's network must be authorised and meet all required standards. Failure to do so will result in immediate disconnection.

Security of Assets

All major IT assets should have a nominated owner who is responsible for security measures.

Availability of data should be maintained by taking back ups and through provision of Uninterruptible Power Supply (UPS) for key infrastructures such as servers and data warehouses.

Locally based systems are the responsibility of issued person. The Director will provide guidance and advice to ensure that information security meets required standards.

Computer Operations

Responsibilities and procedures for the management and operation of all computers and networks should be established and supported by appropriate documented operating instructions.

Procedures should include: Back-up, media control, event logging, monitoring, protection from theft and damage, unauthorised access and capacity planning.

Systems Development, Planning and Procurement.

Security issues must be considered and documented during the requirements phase and the procurement phase of all system procurements and developments. Minimum security standards will be incorporated in all new systems.

New operational software should be quality assured. System test and live data should be separated and adequately protected. All changes to the systems must pass through a formal change control procedure.

Legal Requirements and Regulations

- Physiotherapy2fit and all staff are governed by laws & regulations including, but not limited to:
- Data Protection Act 1998.
- Data Protection (Processing of sensitive Personal Data) Order 2000
- Copyright, Designs and Patents Act 1990.

- Computer Misuse Act 1990.
- Freedom of Information Act 2000.
- Access to Medical Records Act1988.
- Access to Health Records Act 1990
- Report on the Review of Patient - Identifiable Information (Caldicott Report) December 1997.
- Human Rights Act 1998.
- ISO/IEC 27001
- NHS Confidentiality Code of Practice 2003
- NHS Code of Practice on Information Security Management 2007
- GDPR legislation

More information is available in the relevant policy (for example the Data Protection Policy) technical details may be found in the IM&T Security Policy, and further advice may be obtained from the Head of Information Governance.

The intellectual property rights over any software developed on Physiotherapy2fit equipment by staff employed by Physiotherapy2fit, belongs to the Physiotherapy2fit unless explicitly covered by a separate agreement.

Unauthorised or unlicensed software is not permitted on Physiotherapy2fit equipment. It is expressly forbidden for any user to load or operate software gained from the Internet, magazine gifts or other sources unless authorised by the Director of Physiotherapy2fit.

Business Continuity Planning

Physiotherapy2fit has processes in place to develop and maintain appropriate plans for the speedy restoration of all critical IT systems. All systems will have threats and vulnerabilities assessed to determine how critical they are to Physiotherapy2fit. Individual work areas should have procedures in place to maintain essential services in the event of IT system failure.

Personal Computers

Each PC (including notebooks, laptops, palmtops, portables), shall have a designated system owner responsible for overall security on the system. PCs shall be specified and purchased in accordance with current recommendations on software and hardware.

Precautions must be taken to prevent and detect computer viruses. The Director manages antivirus software and seek advise from the CCG on virus control.

If sensitive information is present on the PC, then the advice and agreement from Physiotherapy2fit should be obtained before the PC is taken off site or used outside of a secure area.

Personal Use

Personal use of IT equipment is permitted providing that it is done with Director approval, it is not in support of a business, it does not use excessive system resources and it is done in the employees own time. Consumables must be paid for.

Encryption

All person identifiable data will be transmitted/transported either in an encrypted format or via secure e-mail. Where this is not possible, a risk assessment will be conducted and approved by the director.

Implementation and Monitoring Plans

The Information Governance Committee is responsible for this policy and will ensure the necessary reviews and updates in accordance to changes in national policy or legislation. Monitoring of this policy will be through the annual assessment required by the Information Governance Toolkit, led by the Director.