NORTHUMBERLAND HEATH MEDICAL CENTRE

Hind Crescent, Northumberland Heath, Erith, Kent. DA8 3DB

INFORMATION SECURITY POLICY

Created by	S Flanagan	December 2012
Agreed by	Dr M McIntyre	December 2012
Reviewed by	B Russell	May 2020
Next Review Date		May 2021

1. Introduction

This information security policy shall apply to information, systems, networks, applications, locations and staff of [the practice]. It is based on the expectations set out within the Information Security Management: Code of Practice for NHS organisations (see https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice).

The purpose of this policy is to enable and maintain effective security and confidentiality of information processed or stored by Northumberland Heath Medical Centre. This shall be achieved by:

- Ensuring that all members of Northumberland Heath Medical Centre staff are aware of and shall comply with relevant legislation, including the Data Protection Act (1998) and the Data Protection (Processing of Sensitive Personal Data) Order 2000.
- Describing the principles of information security management and describing how they shall be implemented within Northumberland Heath Medical Centre
- Introducing an approach to information security that is consistent with other NHS organisations.
- Assisting staff to identify and implement information security as an integral part of their day to day role within the practice.
- Safeguarding information relating to staff and patients under the control of the practice.

2. Objectives

Key objectives of this Northumberland Heath Medical Centre Information Security Policy are to preserve:

- **Confidentiality** - Access to information shall be restricted to those GPs and staff of Northumberland Heath Medical Centre and relevant others with agreed authority to view it.

- **Integrity** – Records are to be complete and accurate with all filing and management systems operating correctly.
- **Availability** - Information shall be readily available and delivered to the authorised GP or medical professional, when it is needed.

3. Responsibilities for Information Security

- Responsibility for information security shall rest with the Senior Partner However, on a day-to-day basis the Practice Manager shall be responsible for organising, implementing and managing this policy and its related good working practices.
- The Practice Manager shall be responsible for ensuring that both permanent and temporary staff including any contractors and locums are aware of:-
  - The information security policies applicable to their work areas
  - Their personal responsibilities for information security
  - Who to ask or approach for further advice on information security matters.
- All staff shall abide by security procedures of Northumberland Heath Medical Centre This shall include the maintenance of Practice records whilst ensuring that their confidentiality and integrity are not breached [this applies to patient, staff and practice information]. Failure to do so may result in disciplinary action.
- This Information Security Policy document shall be owned, maintained, reviewed and updated by the Practice Manager. This review shall take place annually. The results of which shall be made known to the Senior Partner with overall responsibility for security.
- Staff of Northumberland Heath Medical Centre shall be responsible for both the security of their immediate working environments and for security of information systems they use [eg workstations, laptops, PDAs, etc].
- Any contracts with third party organisations that allow access to the information systems of Northumberland Heath Medical Centre shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies / guidance required by Northumberland Heath Medical Centre.

The Practice shall undertake to ensure:

1. **Contracts of Employment –** address information security requirements at the recruitment stage and that all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.

2. **Access Controls -** to areas containing information systems are restricted and controlled to ensure that only GPs and those authorised can access information of the Practice.

3. **Equipment Security –** is effective in order to minimise losses, or damage to the Practice. All information assets and equipment shall, where possible be physically protected from security threats and environmental hazards. (Locked cabinets (fire proof if possible), clear desk policy and the limitation of risks in the surrounding work area etc).

4. **Information Risk Assessment –** a regular assessment of the working environment, shall be conducted to identify potential risks to the security of Practice information. Where risks are identified, these should be noted and where possible mitigating action taken.

5. **Security Incidents and weaknesses -** are to be recorded and reported to the senior partner responsible for security so that they can be investigated to establish their cause, impact and the effect on the Practice and its patients. (NB. remedial changes arising may need to be included within future staff working procedures, updates to policies and contracts of employment).

6. **Protection from Malicious Software –** should be provided through the use of commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of the Practice without the explicit permission of [name/role]. Breach of this requirement may be subject to disciplinary action.

7. **Secure Communications –** should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of patient records are conducted in a secure and confidential manner. The communication of NHS Confidential or NHS restricted information by email must be appropriately protected, using cryptographic controls (AES 256 bit or equivalent). NB: When using NHSmail this technical security protection is automatic.

8. **Business Continuity and Disaster Recovery Plans –** are in place so that in the event of a disruption to the information services of the Practice, it is possible to activate relevant business contingency plans until affected services are restored.