DATA & INFORMATION SECURITY POLICY

Chevin Medical

Created by DPO and reviewed by DM 30.3.20

Executive Summary

This document defines the Information Security Policy for the Practice

It is intended to set out Practice policy for the protection of the confidentiality, integrity and availability of information assets including hardware, software and data handled by information systems, networks and applications. It also relates to paper-based information assets and verbal communications. The document establishes the security responsibilities of employees, systems and technical controls required to mitigate against risks to data security.
References are provided for other related documentation.

The document is a requirement of the Data Security and Protection toolkit (DSPT).

Equality Statement

This policy applies to all employees of Chevin irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1. INTRODUCTION

This document defines the Information Security Policy for the Practice

The Information Security Policy applies to all business functions and information systems, networks, physical environment and relevant people who support those business functions.

This document:-

- Sets out the Practice's policy for the protection of the confidentiality, integrity and availability of its information assets including hardware, software and information handled by information systems, networks and applications.
- Also relates to manually held information assets and verbal communications.
- Establishes the security responsibilities of information security.

- Provides reference to documentation relevant to this policy.

2. AIMS

The objective of this policy is to enable the Practice to protect its information assets by:

- Setting out a framework for information security
- Promoting a culture of information security best practice across the organisation and its partners
- Ensuring staff understand their responsibilities

Application of the information security policy will ensure that:

- Each Information asset has been assigned an Information Asset Owner
- Information is protected against unauthorised access and/or misuse
- The confidentiality of information is assured
- The integrity of information is maintained
- Information is available when and where required
- Business Continuity Plans are produced, maintained and tested.
- Regulatory, legal and contractual requirements are complied with
- Appropriate training is provided to all staff
- Breaches of Information Security are reported and investigated
- The physical and environmental aspects of information security are considered and managed

The Information Governance Strategic Vision, Policy and Framework acts an overarching policy for the core information governance polices. The Information Security Policy is one of those core policies and must be read in conjunction with the overarching Policy. Additionally, procedures will be produced to support this policy and should also be read in conjunction with the other information governance and security related policies including the Network Security Policy (see Section 12 Associated Documents).

3. SCOPE

This policy must be followed by all staff who works for or on behalf of the Practice including those on temporary or honorary contracts, secondments, volunteers, pool staff, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the Practice. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

3.1 Systems and Devices

- All manual and electronic information systems owned, operated or managed by

the Practice and its Information Technology provider, including networks and application systems, whether or not such systems are installed or used on Practice premises.
- Other systems brought onto Practice premises including, but not limited to, those of contractors and third party suppliers, which are used for Practice business.
- Desktop devices used to hold Practice information such as Laptops, mobile phones, tablets, Apple and Android devices,
- Portable devices used to hold information such USB memory sticks or external hard drives

3.2 Information

- All information collected or accessed in relation to any Practice activity whether by Practice employees or individuals and organisations under a contractual relationship with the Practice.
- All information stored on facilities owned, leased or managed by the Practice or on behalf of the Practice.
- Information processed by the Practice including the transmission, printing, scanning of that information.
- Information processed by a contractor organisation on the Practices behalf and which is held on non–Practice premises (more detail on this area can be seen in the Practice Records Management and Information Lifecycle Policy)

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

4. ACCOUNTABILITY AND RESPONSIBILTIES

There are a number of key information governance roles and bodies that the Practice needs to have in place as part of its Information Governance Framework, these are:

- DPO
- Partnership Committee
- Governance, Performance and Risk Committee
- Caldicott Guardian
- Information Asset Owner/Administrator
- Heads of Service/department
- All employees

The accountability and responsibility are set out in more detail in the Information Governance Strategic Vision, Policy and Framework which must be read in conjunction with this policy.

5. DEFINITION OF TERMS

The words used in this policy are used in their ordinary sense and technical

terms, where ever possible, have been avoided.

6. ENSURING THAT INFORMATION IS SECURE

The sections below set out the conditions for ensuring security of information for specific work situations, work areas, equipment and media.

6.1 Processes for the security of Equipment and Records

- In order to minimise loss of or damage to all assets, all equipment and all information storage areas must be physically protected from security threats and environmental hazards.
- Confidential information held in hard copy (paper) must be kept secure at all times e.g. locked in a cabinet when not in use.
- Personal and confidential information must not be stored on local hard drives such as those on PCs, laptops, other portable devices or in online storage unless authorised.
- Any personal, confidential or sensitive information held on portable devices must be encrypted.
- Databases of personal information containing service user information and staff information must not be created without prior permission.
- All databases of information must be included on the Information Asset Register part of which will include risk assessments and business continuity planning.
- Information Asset Owners are responsible for ensuring the physical and environmental security of information systems for which they are responsible.
- For information that does not contain personal or confidential details which may be the case for most business organisational records, staff will still need to process these records securely. Access to these types of records by staff or by partner organisations will be dictated by a staff member's agreed duties and organisational business needs. Access in the wider context such as in the public domain will be dependent on legislative requirements.

6.2 Location and Physical Access Controls

- Only authorised personnel who have an identified need are given access to restricted areas containing information systems such as the server room or a file store room.
- There will be appropriate access controls in place at Practice premises e.g. access to the building controlled by code entry, or reception controlled access.
- Non-Practice staff need to sign on the Practice reception register when working on Practice premises.
- All staff need to wear an identification badge at all times when on Practice premises.
- Staff should challenge individuals who they do not recognise, do not have an ID badge and who does not appear to be working for or with any particular section or team.

6.3 User Access Controls

- Access to information and information systems, whether electronic or manual, is restricted to authorised users who have an identified need as agreed with their line manager, sponsor and/or Information Asset Owner.
- Access to electronic information systems is given at the appropriate level for the agreed need by the appropriate Information Asset Owner.
- Information Asset Owners should review whether staff should have access (or be granted access) to an information system. This process needs to be recorded and included in the Information Asset Register against the appropriate information asset.
- Where staff members leave or move to another section, their access to any relevant information systems must to be revoked by the Information Asset Owner where that access is no longer justified.
- Person confidential data may only be stored within a secure environment on operational systems within a safe haven i.e. there is restricted access and technical security relative to the sensitivity of the information.

6.4 Password Protection

The primary form of access control for the Practice's computer systems is via password. Each member of staff using a computer system will have an individual password.

Sharing of passwords by both the person who shared the password and the person who received it is an offence under the Computer Misuse Act 1990. All staff must follow robust security practices in the selection and use of passwords. Logon details are not to be shared or used under supervision, even in training situations. Staff will be held responsible for any action undertaken with their login credentials.

6.5 National Applications Systems Controls

National applications include systems, services and directories that support the NHS in the exchange of information across national and local NHS systems e.g. Summary Care Record, e-Referrals, etc.

National Spine-enabled systems are controlled by a number of different security mechanisms (these are listed below).

The range of access controls applied by national applications include:

- Smartcard: access will be restricted through use of an NHS Smartcard with a pass code, provided by the local Registration Authority. Access will be monitored by the practice in relation to role based access, audit of access and alerting to potential misuse.
- Training*:* access will only be allowed following appropriate training.

- Legitimate relationships*:* Staff will only be able to access patient records if the are required to do so for that patient's care.
- Role Based Access Control (RBAC)*:* access will depend on staff roles/job/position functions. Roles and access privileges will be defined centrally and given locally by staff designated to do this in the organisation.
- Audit trails*:* an electronic record will be made automatically of who, when and what information a user accessed. Trails can be assessed by an appropriately authorised manager.
- Alerts*:* alerts will be triggered automatically both to deter misuse of access privileges and to report any misuse when it occurs.

6.6 Connection to the Practice Network

This is covered in the Practice **Network Security Policy** which should be read in conjunction with this policy.

6.7 Remote Working

- Work related information that is taken off site must be authorised by line management, protected by proper security and, where held on portable computers or devices, backed up regularly to the appropriate Practice server or system. Portable devices must be used in line with Practice procedures and protected by appropriate security and encryption (See section on Portable Devices).

- It is recognised that remote login/desktop provides an option whereby the need to transport information is removed. Working remotely must be authorised by line management and comply with the full suite of policies relating to Information Governance.

6.8 Portable/Personally owned Devices

- The use of portable devices (that include Laptops, mobile phones, smartphones/tablets, USB memory sticks) for work purposes must be in line with Practice policy and authorised by your line manager (and the Practice IT Services provider, where appropriate).

- Only portable devices that meet the requirements of this policy and all NHS requirements may be used for work purposes.

- Personally owned portable devices such as Laptops, smart phones, smartphone/tablet devices should not contain work related information/information assets and must not be directly connected to the corporate network either by a direct network cable connection or Wi-Fi connection. However, such devices may be connected to the Practice 'guest' Wi-Fi service but only if in accordance with the full suite of information governance policies.

- Portable storage devices (including CDs, DVDs, USB and flash drives)

containing software or data from external sources, or that have been used in external equipment, must be fully virus checked before being used on the Practice network.

- All portable devices, including storage devices, must be encrypted to NHS standards and, where appropriate, have up to date antivirus software.

- Portable devices used to access NHS Mail must be encrypted to NHS Mail standards and have the capacity, and be configured, to allow remote wiping.

- All security and encryption features on portable devices must be utilised such as username and password authentication. Where additional safeguards can be put in place they must be done so such as a minimum 4 digit PIN being allocated to a mobile phone.

- Where staff leave the Practice, they must return any equipment provided by the Practice.

6.9 Malicious and Unauthorised Software

This is covered in the **Network Security Policy** which must be read in conjunction with this Policy.

6.10 New and Changed Information Systems

Where a new information system is been considered for introduction or there are to be changes made to an existing system then the Practice will use risk analysis techniques to ensure that any new system meets information security requirements. Specific measures and procedures need to be in place to ensure the system is lawful and secure, they include:

- Effective security counter measures
- Relevant security documentation
- Security operating procedures
- Security contingency plans

A Data Protection Impact Assessment (DPIA) should be undertaken as part of an overall project plan. A DPIA will identity any risks and issues that may compromise security and confidentiality and which then can be then be addressed.

The Information Asset Owner will have responsibility for the security of designated information assets and need to be aware of and in agreement with any proposed changes to an existing system or where a new system is being introduced. They will need to assure the IG leads within the practice that the changes or introduction of a new system comply with legislation and that the necessary technical and organisational measures are in place to ensure security.

The Information Asset Register is a record of all key information resources held by the Practice. More detailed information about what information is recorded in the Register is set out in the **Records Management and Lifecycle Policy**.

6.11 Data in Transit and Safe Transfer of Information

When transferring information staff need to take into account the nature of the information to be transferred and ensure that it has the necessary protection to ensure its security. This is especially important when information contains personal, confidential or particularly sensitive information. The section below sets out different types of transfer and security requirements.

6.11.1 Non Routine Bulk Transfers

Any non-routine bulk extracts (50+ records) or transfers of personal confidential or sensitive data must be authorised by the responsible manager or the Information Asset Owner for the work area- see the Records Management and Lifecycle Policy for further guidance.

6.11.2 Transfer by Portable Devices

See section 6.8 above

6.11.3 Transfer by FAX

Transfers of personal, confidential or sensitive information by fax should be avoided and only used where there is no alternative. Where it is necessary to send this type of information by fax, safeguards must be applied in order to ensure the security and confidentiality of the information.

6.11.4 Transfer by the Secure File Transfer (SFT) Service

The SFT is designed to target data transfers between a minimum of 20MB (currently NHS Mail maximum) up to 2GB. This mechanism is to remove the insecure usage of physical media transfer methods, such as:

- CD or DVD
- Memory sticks, USB pen drives
- Printouts

Guidance on using the service can be found at:

https://nww.sft.nhs.uk

6.11.5 Transfer of Data Outside the UK

Consult with the relevant contact (see Section 11) when considering any transfer of personal, confidential information outside the UK to ensure security of the information (see the Confidentiality and Data Protection Policy for details).

Due to the increased uncertainty (at the time of writing) regarding the repercussions of the UK's exit from the EU and the associated risks with the UK no longer having GDPR "equivalency" and proposed transfer of data outside the UK should be discussed with the relevant contact (see Section 11).

6.12 Information Security in the Work Environment

- Under no circumstances should personal confidential information be left out in the open e.g. on an unattended desk or on a computer screen or any place visible to the public.

- Where rooms or cabinets containing records are left unattended, they must be locked.

- Personal confidential information should be stored securely in either a locked cabinet or within a secure environment on a computerised system.

- When leaving your desk for any period of time lock your computer screen using the Ctrl/Alt/Delete facility or Windows Key L . Log off and shut down the computer when you have finished using it.

- When storing electronic records, care must be taken to ensure that no personal identifiable information e.g. health records, human resources records etc., are stored in public folders or on the local drive of the computer.

- Electronic records need to be stored within a folder that can only be accessed via a Practice network drive. The nature of the information can dictate the level of access to that folder (additional security can be applied via a password requirement for further restrictions on access). For information on restricted access settings staff should contact the Practices IT Service Provider.

- Where staff members have concerns about access to certain folders, they should raise the matter with the appropriate Information Asset Owner.

- Where staff print off, scan, fax or copy information they must always make certain the information is collected and not left on the equipment.

- Confidential waste needs to be put in designated bins (in preparation for secure shredding).

- Care must be taken when having conversations in the work environment that may involve personal and confidential information.

6.13 Secure Disposal and Re-use of Equipment

All users must ensure that, where equipment is being disposed of, all data on the

equipment (e.g. on hard disks or portable media) is securely destroyed; this can be arranged by contacting the Practices IT Service Provider. Equipment must be assessed for re-use before being given to a new user or being disposed of.

For disposal of paper records see the **Records Management and Lifecycle Policy**.

6.14 Email Security

See the Practice Email Policy.

6.15 Internet Security

Internet security and usage is detailed in the Practice Internet and Social Media Policy. It is a requirement that all new staff have to have read and understood the Internet Policy before internet access is provided.

7. ORGANISATIONAL CONTROLS AND PROCESSES

7.1 Monitor System Access and Use

Audit trails of system access and use should be maintained and reviewed on a regular basis by the associated Information Assess Owner.

7.2 Business Continuity

The Practice will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks. These form part of the Practice's formal Business Continuity plans.

7.3 Incident Reporting

- All information management and technology security incidents and weaknesses must be reported via Practice incident reporting procedures.
- All security incidents resulting in an actual or potential breach of confidentiality must be reported in accordance with policies and procedures including notification to the Caldicott Guardian as appropriate.
- The Information Asset Owner should conduct a risk assessment where an incident relates to information that falls under their responsibility to ensure that any risk associated with a particular Information Asset is effectively managed
    - Any information governance related incident especially related to a breach of the Data Protection Act that has the potential to be classed as a Information Governance and Cyber Security **S**erious **I**ncidents **R**equiring **I**nvestigation will need to be logged on the Incident Reporting Module on the Data Security Protection Toolkit. Examples of SIRIs are when there is a loss of personal data involving many individuals or where particularly sensitive personal information is lost or sent to the wrong address.

Staff must read the Incident Reporting Policy for general reporting of incidents

and the process for Information Governance and Cyber Security Serious Incidents Requiring Investigation.

7.4 Risk Assessments

The Practice will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all information systems, applications and networks that are used to support those business processes. The risk assessment will identify the appropriate security counter measures necessary to protect against possible breaches in confidentiality, integrity and availability. Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the Practice's risk register and action plans shall be put in place to effectively manage those risks.

The Risk Management Strategy should be read in conjunction with this section.

7.5 Technical Compliance Checking

The Practice Management team will seek assurance from the IT service provider that information systems are regularly checked for compliance with security implementation standards.

8. TRAINING

Information governance and security will be a part of induction training and is mandatory for all staff. The information governance training needs of key staff groups is specified in the IG Training Strategy, which takes into account roles, responsibilities and accountability levels and will review this regularly through the Personal Development Review processes.

It is a line management responsibility to ensure that all staff are made aware of their information security responsibilities through generic and specific staff training.

9. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Practice's IG/Management Team this policy will be disseminated to staff via an appropriate medium e.g. the Practice's Intranet or communication through in-house staff briefings.

This Policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

10. MONITORING EFFECTIVE AND COMPLIANCE OF THIS POLICY

An assessment of compliance with requirements, within the Data Protection and Security Toolkit (DSP), will be undertaken each year- this includes Confidentiality and Data Protection.

All serious information governance incidents must be reported.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity through the Report NHS Fraud website www.reportnhsfraud.nhs.uk or telephoning 08000 28 40 60.

11. ADVICE

Advice and guidance on any matters stemming from the policy can be obtained by contacting your line manager .

12. ASSOCIATED DOCUMENTS (Policies, protocols and procedures)

The Practice will produce appropriate policies, procedures and guidance relating to records management as required. This will include an Information Governance handbook which will be updated annually and which will be given to all staff.

This policy should be read in conjunction with;

- Confidentiality and Data Protection Policy
- Information Governance Strategy
- Information Governance Policy and Management Framework
- Freedom of Information Act and Environmental Information Regulations Policy
- Records Management and Information Lifecycle Policy
- Network Security Policy
- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Plan
- Anti-Fraud and Bribery Policy
- Whistle Blowing Policy
- Internet and Email Policies and Procedures

And their associated procedures (including but not limited to)

- Access to Records Procedure
- Information Sharing Protocol
- Freedom of Information Procedures
- Privacy Impact Assessment Procedure
- Remote Access and Home Working procedures
- Safe Transfer Guidelines and Procedure

13. LEGAL REFERENCES AND GUIDANCE

- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
- Audit & Internal Control Act 1987

- Bribery Act 2010
- Caldicott Guidance as updated 2013
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- GDPR/Data Protection Act 2018
- Electronic Communications Act 2000
- Enterprise and Regulatory Reform Act 2013
- Environmental Information Regulations 2004
- Equality Act 2010
- Fraud Act 2006
- Freedom of Information Act 2000
- Health and Social Care Act 2012
- Health and Social Care Information Centre Guidance
- Human Rights Act 1998
- Information Commissioner's Guidance Documents
- ISO/IEC 27001:2005 Specification for an Information Security Management system
- ISO/IEC27002:2005 Code of Practice for Information Security Management
- NHS Act 2006
- NHS Information Security Management Code of Practice 2007
- Prevention of Terrorism (Temporary Provisions) Act 1989 and Terrorism Act 2000
- Privacy and Electronic Communications Regulations 2003
- Professional Codes of Conduct and Guidance
- Protection of Freedoms Act 2012
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulations under Health and Safety at Work Act 1974
- Road Traffic Act 1988
- The Children Act 1989 and 2004Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992