NCEPOD

Information Security, Confidentiality and Data Protection Policy – extracted from the staff handbook

This section should be read in conjunction with the Information Security Procedures, which are reviewed annually. Please ask the IT Manager for the folder detailing all of NCEPOD's security and confidentiality procedures.

4.6.1 The need for a security policy

NCEPOD is committed to ensuring the security of the information it holds. Information is held and processed in two formats: on paper and on its computer system.

Information security can be defined as protecting the confidentiality, integrity and availability of data and information.

- Confidentiality: protecting sensitive information from unauthorised disclosure
- Integrity: safeguarding the accuracy and completeness of information
- Availability: ensuring that information is available to users when required

Information security is vital to the work of NCEPOD for three principle reasons:

1. Confidentiality and security of information is fundamental to the continued success of NCEPOD, through maintaining the confidence of patients, clinicians and hospitals that submit data to the Enquiry.
2. NCEPOD has a legal obligation to maintain security and confidentiality under the Data Protection Act and General Data Protection Regulation which applies to paper as well as electronic information.
3. If data loses its integrity or availability then the work of NCEPOD will be severely compromised.

4.6.1.1 Information Security and BS ISO/IEC 27001:2013 controls

The NCEPOD Information Security Policy and procedures have been formulated in conjunction with the International Standard ISO/IEC 27001:2013 "Information technology – Code of practice for information security management". By using ISO/IEC 27001:2013 to help assess, manage, and review risks, NCEPOD demonstrates its commitment to information security and confidentiality.

Only those controls that have been seen as being relevant to its organisational structure, business functions and goals have been selected by NCEPOD. Appendix F of the Information Security Procedures identifies these controls.

4.6.1.2 Scope of the security policy

NCEPOD’s security policy aims to ensure that:

- All systems, electronic and paper, are properly assessed for security
- Computer systems are properly maintained and monitored
- Confidentiality, integrity and availability are maintained
- Staff are aware of their responsibilities, roles and accountability
- Procedures to detect, report and resolve security breaches are in place
- Procedures for enabling business continuity are in place
- Procedures for regular review of the policy, procedures and infrastructure are in place.

4.6.1.3 Key references

- Ensuring Security and Confidentiality in NHS Organisations (E5501). NHS Executive; January 1999
- Guide to the British Standard Code of Practice for Information Security Management (PD0007). BSI; 1995
- Protecting and Using Patient Information – a manual for Caldicott Guardians. NHS Executive; March 1999
- British Standard BS ISO/IEC 17799:2000 (BS7799-1:2000) Information technology – Code of practice for information security management
- Data Protection Act 2018
- Updated ISO/IEC 27001:2013
- General Data Protection Regulation 2016

4.6.2 Security Management

4.6.2.1 Objective

To establish the management structure for information security within NCEPOD.

4.6.2.2 Allocation of Information Security responsibilities

The Chief Executive, on behalf of the Trustees, will be responsible for the overall implementation and enforcement of the Information Security Policy and will also act as the Caldicott Guardian and Data Controller for NCEPOD. Responsibilities include:

- Ensuring compliance with relevant legislation
- Ensuring compliance with the Policy and procedures
- Ensuring that all staff sign confidentiality undertakings
- Ensuring that the IT Manager is aware of staff changes and access rights
- Ensuring data quality
- Ensuring up to date records management
- Responding to breaches of information security
- Responding to Freedom of Information requests

- Responding to data subject access requests
- Reporting any breaches of security to the Trustees.

The IT Manager is responsible for:

- Ensuring that all staff are trained in the secure use of computer systems and aware of any changes to information security procedures
- Ensuring that no unauthorised access to the computer system is permitted
- Ensuring appropriate levels of access to the computer system are maintained
- Ensuring procedures are in place to minimise the risk of theft/fraud/disruption of systems
- Maintaining an inventory of all hardware and software owned by NCEPOD
- Ensuring the appropriate administration of password protection
- Administering the NCEPOD computer network.

All staff are responsible for:

- Operating within the parameters laid down in the NCEPOD information security procedures
- Ensuring that no breaches of information security result from their actions
- Reporting any security incidents or queries to the IT Manager.

The Chief Executive, IT Manager, and Clinical Researchers form the NCEPOD Information Security Forum. This forum meets quarterly and is responsible for the operational management of the security system, including:

- Monitoring and reporting on the state of information security within NCEPOD
- Ensuring that the Information Security Policy is implemented throughout NCEPOD
- Developing detailed procedures to maintain security
- Ensuring that staff are aware of their responsibilities for information security
- Monitoring for actual or potential breaches of information security
- Approving major initiatives to enhance information security
- Reviewing and approving the Information Security Policy and overall responsibilities.

4.6.2.3 Review and audit

The Policy, its implementation and systems, will be subject to regular review by the Information Security Forum, utilising external support and advice where necessary.

4.6.3 NCEPOD Information Security Key Points

The following points are intended to reinforce and not replace the NCEPOD Information Security Procedures. The relevant sections of the security procedures should be still read and understood by all staff. References in brackets relate to the appropriate section in the procedure document.

4.6.3.1 Locking Workstations (20.4.7)

Machines must not be left unattended in an unlocked state. Press CTRL-ALT-DEL and select 'Lock Computer' to lock a machine.

4.6.3.2 Password Policy (11.4)

Passwords are changed every 60 days; the system enforces this. Passwords should never be told to another person or recorded anywhere. Passwords should contain both letters and numbers and be at least 8 characters in length. Sensitive information that is sent/taken outside of the NCEPOD network must be password protected with the recipient being informed verbally of the password used.

4.6.3.3 Virus Policy (15.4)

Unauthorised software should not be installed or executed on any computer on the NCEPOD network, including patches or upgrades, without the permission of the IT Manager. Any suspected or actual virus infection should be reported to the IT Manager as soon as practical.
The installation of antivirus software on machines on the NCEPOD network should not be interfered with.

4.6.3.4 Unsolicited Email Policy (17.3.6)

All unsolicited or suspicious email should be moved to the Spam Email folder immediately.

4.6.3.5 E-mail protocols (17.3)

NCEPOD provides electronic mail for business communications, to be used in performing assigned job duties. Staff should fully familiarise themselves with the guidelines for appropriate usage outlined in Sections 17.3.1 to 17.3.7, and Section 19.4, of the Information Security Procedures.

Inappropriate use of email may result in disciplinary action being taken. Flagrant abuse of NCEPOD's email policy is treated as gross misconduct. NCEPOD reserves the right to monitor email usage to ensure that official NCEPOD policy is not contravened or abused.

Emails have become an accepted method of both internal and external communications, often replacing the "written" letter and memo. The informality and ease of use of e-mail is its virtue but it is necessary to ensure that this informality is not viewed by colleagues or external contacts as unprofessional, and of a lesser standard than would be adopted for letters and memos. It is important to remember that the content of emails are regarded as a form of publication and are subject to the law of libel.

The following protocols have been defined for use by all staff to ensure clarity and professionalism in all our communications:

- Do not assume that the recipient will be able to identify you from your name. Unless you are confident then you should state your name and title, and whether you are writing in your own name or on behalf of a colleague
- Be professional when sending e-mails. Remember that emails can be printed and retained
- Be clear whether you are providing information or requiring a response and, if so in what timescale
- Emails are not guaranteed to reach the destination that they are intended for. If the content of the email is important, and requires a response, it may be wise to follow up the email with a phone call, or to send a copy of the information sent via the regular post
- Always check the spelling and readability. An informal note should not be mis-spelt or be ungrammatical
- Always use the "signature" included in the NCEPOD email template on all emails. "This email contains information intended for the addressee only. It may be confidential and may be the subject of legal and/or professional privilege. Any dissemination, distribution, copyright or use of this communication without prior permission of the addressee is strictly prohibited. If you have received this in error, please contact the sender and delete the material from your computer".
- Do not use the email facilities to distribute any material that is illegal, pornographic, racist, sexist or likely to cause offence in any way nor any material which may harm the organisation's reputation. NCEPOD will regard any such activity as a disciplinary offence to be dealt with through the standard disciplinary procedures.

4.6.3.6 Data Protection (18.0)

The General Data Protection Regulation 2016 (GDPR) gives certain rights to individuals about whom information is held (manually or electronically). Individuals may ask for information about themselves, challenge it if appropriate or request that their data be omitted from processing. The GDPR places responsibilities on those organisations as both controllers and processors who record and use personal data.

The GDPR contains six data protection principles that organisations should work to:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

The principle of accountability also applies to data controllers who should be able to demonstrate that they comply with these principles.

The risks to the organisation of failing to comply with the requirement of the Act are clear. Not only is there risk of criminal sanctions but also the risk of public embarrassment over failure to comply. It is also worth remembering that where an offence under the Act is committed by an organisation any employee is personally liable if the offence is attributable to neglect on their part.

4.6.3.7 Subject Access (18.1)

All subject access requests should be referred to the Chief Executive. Responses will be made within a month of request. There will be no charge for data access.

4.6.3.8 Compliance (ISO 12) (28.0)

NCEPOD acknowledges the importance of complying with all appropriate criminal and civil law, regulations or contractual obligations. NCEPOD gives full consideration to this when designing the procedures for NCEPOD's information processing facilities and in all data handling tasks seeks to comply fully with the appropriate regulations.

The Chief Executive, on behalf of the Trustees, is responsible for ensuring compliance with all relevant legislation. All relevant statutory, regulatory and contractual requirements are taken into account when designing and documenting information systems and processes. Any specific controls and individual responsibilities necessary to meet these requirements are similarly defined and documented.

All new legal, regulatory and contractual agreements will be reviewed for any necessary changes to the security policy.

NCEPOD is registered as a Data Controller. The Chief Executive, on behalf of the Trustees, has responsibility for compliance with the General Data Protection Regulation.

NCEPOD complies with the legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, and trademarks. NCEPOD complies with legal restriction on the use of licensed software, and promotes an internal policy of legal usage.

All legal, statutory or regulatory requirements for maintaining records are complied with. Information is classified by type, and this classification is used to ascertain the necessary period of retention (in conjunction with the guidelines for retention of data given in Appendix E of the Information Security Procedures). All organisational records are securely stored to prevent loss or destruction to important and sensitive information.

Where any action to be taken involves the law, either civil or criminal, NCEPOD will conform to the rules of evidence as laid down in the relevant law, or in the rules for the specific course in which the case will be heard. NCEPOD will take relevant advice on each individual matter, covering the admissibility, quality and completeness, and consistency of the evidence.

The information processing facilities provided by NCEPOD are for business use. NCEPOD reserves the right to monitor use of the facilities to detect and prevent improper usage.

Where any targeted monitoring takes place, the staff member(s) involved will be informed prior to the monitoring occurring.

Where appropriate, a message will be prominently displayed at the log on stage indicating that the system being entered is private and that unauthorised access is not permitted.

4.6.3.9 Personnel security (29.0)

To reduce the risks of human error, theft, fraud or misuse of facilities, NCEPOD addresses security considerations at the recruitment stage, and within staff contracts.

Verification checks are made at the time of job application for permanent staff positions (Section 29.2 of the Information Security Procedures). Screening should be carried out for contractors and temporary staff, where they will be handling sensitive information. Where temporary staff are provided through an agency, the contract with the agency should clearly specify the agency's responsibility for screening and the notification procedure they need to follow if screening has not been completed or if the results give cause for doubt or concern.

Management should evaluate the supervision required for new and inexperienced staff with authorisation for access to sensitive systems.

All staff are bound to confidentiality, and to the terms of the NCEPOD Information Security Policy, by the Terms and Conditions of their employment. The Terms and Conditions, in conjunction with the Staff Handbook, spell out the employee's rights and responsibilities.

END