SOUTH DURHAM HEALTH CIC

INFORMATION SECURITY POLICY

DOCUMENT CONTROL

Confidentiality Notice

This document and the information contained therein is the property of South Durham Health

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from South Durham Health.

Document Details

Classification:	Standard Policy Document
Author and Role:	Jill Moulton - Chief Executive (to April 2021)
Organisation:	South Durham Health
Document Owner	Susan Watson – Chief Executive (from May 2021)
Document Reference:	72.2018 Information Security Policy
Current Version Number:	0.1
Current Document Approved By:	Board
Date Approved:	23/03/2018

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
0.1	12/02/2018	JM	Board	Reviewed with DPO July 2018
0.2	15/06/2022	SW	KS	Reviewed – no changes made
0.3	21/06/2022	SW	KS	Reviewed and section regarding record retention added.
0.4	20/06/2023	SW		Policy reviewed – no changes made

Policy

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of South

Durham Health's information. It is the overarching policy for information security and supported by specific technical security, operational security and security management policies. It supports the 7 Caldicott principles and 10 data security standards. This policy covers:

- Information Security Principles.
- Governance – outlining the roles and responsibilities.
- Supporting specific information security policies – Technical Security, Operational Security and Security Management.
- Compliance Requirements.

Information Security Principles

The core information security principles are to protect the following information/data asset properties:

- Confidentiality (C) – protect information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.
- Integrity (I) – retain the integrity of the information/data by not allowing it to be modified.
- Availability (A) – maintain the availability of the information/data by protecting it from disruption and denial of service attacks.

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A properties are breached.

The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.

For the NHS, the core principles are impacted, and the effect aggregated, when any data breach relates to patient medical data.

Governance – Roles and Responsibilities
All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting South Durham Health business. All staff are responsible for information security and remain accountable for their actions in relation to NHS and other information and information systems. Staff shall ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is accountable for information risk within South Durham Health and advises the Board on the effectiveness of information risk management across the organisation.

All Information Security risks shall be managed in accordance with the South Durham Health Risk Management Policy.

Service Lead Managers shall:

.

- Ensure the operational effectiveness of security controls and processes.

- Be accountable to the SIRO and other bodies for Information Security across South Durham Health.
- Monitor potential and actual security breaches with appropriate expert security resource.

Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.

Data Protection Officer

SDH will secure access to a DPO in line with the requirements of the General Data Protection Regulation

- The GDPR makes it a requirement that organisations appoint a data protection officer (DPO) in some circumstances.
- The GDPR also contains provisions about the tasks a DPO should carry out and the duties of the employer in respect of the DPO.

- A DPO must be appointed by public authorities (except for courts acting in their judicial capacity) and those who carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

  A data protection officer may be appointed to act for a group of companies or for a group of public authorities, taking into account their structure and size.

  Regardless of whether the GDPR obliges an organisation to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

  The DPO's minimum tasks are defined in Article 39:

  - To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
  - To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
  - To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

  - The DPO must report to the highest management level– ie board level.
  - The DPO operates independently and is not dismissed or penalised for performing their task.

Information Asset Owners

The Information Asset Owners (IAOs) are senior/responsible individuals involved in running the business area and shall be responsible for:

- Understanding what information is held.
- Knowing what is added and what is removed.

- Understanding how information is moved.
- Knowing who has access and why.

Senior Responsible Owners

All Senior Managers, Information Risk Owners and Directors, defined as Senior Responsible Owners (SROs), are individually responsible for ensuring that these policy and information security principles shall be implemented, managed and maintained in their business area. This includes:

- Appointment of Information Asset Owners (IAO) to be responsible for Information Assets in their area(s) of responsibility.
- Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks
- Supporting personal accountability of users within the business area(s) for Information Security
- Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures.

Staff Responsibilities

- Each employed, contracted and voluntary staff member is personally responsible for ensuring that no breaches of information security result from their actions
- Attend relevant information security/governance training to ensure that are fully aware of their personal responsibilities in respect of information security, and that they are competent to carry out their designated duties
- Fully comply with the Company's Information Security policy and all relevant security policies and procedures
- Understand that beaches of this policy will be investigated by formal disciplinary procedure which may lead to dismissal and/or legal action
- Understand they are personally responsible for the accuracy of information/data recorded
- Ensure they are familiar with safe haven procedures for secure transportation of information
- As part of their contract of employment sign a formal undertaking concerning the need to protect the confidentiality of information / observe intellectual property rights of work undertaken during the terms of employment / contract, both during and after contractual relations with the Company.

Training/Awareness

All staff are mandated to undertake Information Governance training and where appropriate in depth information security training to ensure that they fully understand and are aware of this policy, its requirements and the obligations it places on them as a member of Company staff.

Training for staff will include the use and protection of both paper and electronic records systems.

Training requirements will be regularly assessed and refreshed in order that staff may remain appropriately skilled/ knowledgeable over time.

Information Risk Management

Information risk is inherent in all administrative and business activities and will be managed in a structured way through the Company's current risk management framework.

Effective information security management is based upon the core principle of risk assessment and management. This requires the identification and quantification of information security risks in terms of their perceived severity of impact and the likelihood of occurrence.

The risk assessment management structure and processes identify how information-related risks are controlled. Reviews of implemented information security arrangements are an essential feature of an organisation's risk management programme.

Once identified, information security risks will be managed on a formal basis through the Risk register and monitored by the Board. Risks will be recorded within a Company risk register and action plans will be developed to demonstrate the Company's effective management of its information assets risks.

The Company's Risk register and all associated actions will be reviewed at regular intervals.

The Company's SIRO, IAO's and IAA's will work together to manage the Company information security risks within the Company's current risk management structure and arrangements.

Information Assets

The Company's information assets will come in many different forms. Below is an example of the Company's information:

Personal Information	**Software**
Staff /Contractors records Clinical Audit Data Research Data Management / Performance Data Company Membership records	Clinical Systems software Microsoft Office software Applications software System Software
System / Process Documentation	**Hardware**
System information / Support documentation Information databases Data files / Archive data / information Audit data	PC's/Computers Laptop USB sticks Printers, Scanners
Corporate Information	**Miscellaneous**
Meeting Minutes / Papers Financial information Company Policies / Procedures / Guidance Presentations Company Reports / Returns Operational Procedures / Manuals Contracts / Service Level Agreements	Staff skills / Experience / Knowledge

The Company Information Asset list will be managed and maintained by the Chief Executive in liaison with the Company's IAOs.

The list will be grouped in a logical order e.g. as per the example table above.

Given the constraints of time and resources, priority will be given to information assets that (a) contain personal information about patients or staff and/or (b) are essential to the support of Company operations, e.g. financial systems, infrastructure documentation.

All information received, and recorded by the Company will have:

- An Owner - i.e. the person that is the business/clinical main user of the information, or the person that acquired the information from a third party
- A Custodian – i.e. the person(s) that processes the information on behalf of the owner according to protocols defined by the owner
- A User – i.e. the person using the information in accordance with legislation and regulation to perform their job functions.

These roles need to be identified when the Information Asset is entered onto the Company's Information Asset Register.

Threats to NHS data shall be appropriately identified and based upon robust risk assessment and management arrangements, and shall be managed and regularly reviewed to ensure:

- Protection against unauthorised disclosure
- Integrity and evidential value of information is maintained
- Information is available to authorised personnel as and when it is required.

Information Security Incident Management

All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

All Company incidents must be reported using the Company incident reporting procedures and managed in line with the Company's Incident Reporting Policy. All incidents must be reported as soon as they are identified.

Where there is an information security breach or event this will be managed by the Service Lead Manager and reported to the Company's SIRO.

Information security incidents will be reported to the Board who will, where applicable, approve changes to Company policies and procedures to reduce the risk of the information security incident reoccurring.]

Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious, and could be reported as a Serious Untoward Incident. This applies irrespective of the media involved and includes both the loss of electronic media and paper records.

Where an information security breach is classified as a Serious Untoward Incident (SUI) this will be reported to the appropriate bodies.

Security of Manual/Verbal Information

Safe Havens

The definition of a safe haven is a secure location where a designated member of staff is responsible for ensuring the secure receipt and delivery of information sent to the Safe Haven.

Service Lead Managers will maintain a list of safe haven areas.

Safe Haven Procedures

Safe haven procedures for all methods of transferring confidential information are in place which staff must follow for:

- Post
- Electronic / Email
- Transporting
- Faxing
- Bulk Transfer

Verbal Information

The Company has a legal obligation to ensure that all personal data being processed is kept secure (Data Protection Act principle 7).

Staff must ensure when holding confidential conversations these are not undertaken in a public area, or where a member of staff who does not need to access to the confidential information can overhear the conversation.

Staff should also take extra care on the positioning of answer phones where messages containing confidential information can be left.

The identity of persons requesting and receiving sensitive or confidential information over the telephone must be verified, and they must be authorised to receive it.

All parties are to be notified in advance whenever telephone conversations are to be recorded.

Clear Desk Policy

The Company must ensure that all confidential information is not left unattended and is removed to a secure location e.g. locked filing cabinets.

Sharing Confidential Information

Where there is a need for staff to share patient information with another NHS organisation, staff must ensure that the sharing of the information complies with both the Data Protection Act 1998 and the Common Duty of Confidentiality.

Sharing of confidential information must comply with information sharing protocols.

Security of Electronic Information

Access Control

The IT Network used by SDH and its subcontractors is NHSE owned and maintained on their behalf by the North East Commissioning Support Unit (NEC and access is in accordance with their policies.

Staff must not attempt to access any part of the network or any IT system to which they are not permitted access.

Where staff have a requirement to access the Company files remotely, this will be in line with the agreement in place with NECS.

Password Management

Staff must not share their passwords with any other member of staff for any reason.

Staff are responsible for changing their passwords when prompted.

Clear Screen Policy
The Company has adopted a clear screen policy, which requires staff to either log off their computer or lock their computer when left unattended for more than 5 minutes.

Where appropriate, the Company will implement the automatic locking of Company computers, after a defined period of inactivity.

Equipment Siting
Whenever IT equipment/IT cables are placed, consideration will be given to both the security of the IT equipment and information to be accessed on the IT equipment. In some instances, IT equipment/rooms will not be named as a security measure.

The correct siting of the IT equipment will reduce the risk of theft and accidental breach/disclosure of confidential information. This could occur through a member of the public being able to view confidential information displayed on the computer screen.

Procurement of IT Systems
Where there is an identified need for a new electronic IT system within the Company this must be agreed with the Board.

All new IT Systems must have approval prior to being purchased to ensure that information security is a fundamental consideration for the IT system design and operation.

A Privacy Impact Assessment must be undertaken against all new systems which will contain personal data. Guidance on completing these privacy impact assessments can be obtained from the Information Commissioner Website.

IT System Operations/Administration
Each Company IT system has a named System Security Manager (Information Asset Administrator) who is responsible for overseeing the day to day security of the systems, which entails:

- Ensuring that system documentation is available and kept up-to-date
- Error/ system logs are reviewed and managed
- Changes to systems operations are fully tested and approved before being implemented,
- Systems scheduling is planned, authorised and documented
- Audit logs are reviewed regularly with discrepancies investigated
- Ensuring only authorised staff or approved third parties may diagnose and correct information system hardware faults.

Electronic Information Management
The day-to-day storage of the Company information will ensure data is readily available to authorised users.

Where data does not need to be readily available, the Company will create data archives. Where information is being archived legal, regulatory and business needs must be considered.

The information created and stored by the Company's information systems will be retained for a minimum period that meets both legal and business requirements

Anti Virus/Spyware/Malicious Code/Mobile Code

Anti Virus software that will be applied to all Company IT equipment, where applicable.

Back-up, Recovery and Archiving.
Arrangements for back up are in place via the company IC support provider.

Staff using laptops or portable computers must ensure that these are connected to the network at least once a month to ensure that the software on the laptop is kept up to date and ensure information held is backed up (e.g. via Offline folders and files).

The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved (e.g. means to read and recover the information must be available during the expected life of the store information).

The archiving of electronic data files must reflect the needs of the Company and any legal and regulatory requirements.

Encryption
To prevent the unauthorised disclosure, modification, removal or destruction of Company information assets and disruption to the Company business, all Company laptops and computers and Mobile telephones and Personal Digital Assistants (PDA's) will be encrypted. Where there is an exception and a genuine business need to not encrypt a Company asset, this must be approved by the Company's SIRO.

Where a member of staff is using non Company equipment for Company business/purpose, this must also be encrypted and kept secure at all times. Unencrypted removable media devices may be used only as temporary storage devices and should hold only a secondary copy of data. Removable media devices must never be used for sensitive data.

Security of IT Equipment
Where a member of staff has been issued with Company equipment, the member of staff is fully responsible for ensuring that the Company asset/equipment is kept secure at all times, not left unattended in a vehicle or in a public place, and locked way when not in use.

Staff are responsible for ensuring that all removable media are kept secure at all times to prevent their loss, damage, abuse or misuse whether stored or in transit.

Where staff are issued with Company equipment, it must only be used for Company business. Where a member of staff wishes to use Company equipment for personal use, the member of staff must comply with all Company policies and be approved by their Line Manager.

When staff are using Company equipment outside of the Company, the member of staff must ensure individuals are not able to see any confidential information e.g. using laptop to access confidential information in a public place (internet café, train, café, home).

If any Company equipment is lost/stolen/missing the member of staff must report the incident to the Company through their Line Manager, and where applicable the Police, as soon as possible.

Destruction of Electronic Data/hardware

The information stored on media must be removed using a destruction method that makes recovery of the data impossible.

This will be managed by the third party contractor NECS) for confidential destruction.

Where staff have electronic hardware that needs to be disposed, this must be passed to the IT Service Desk for confidential destruction.

Forensic Readiness

The universal use of IT systems in the Company leads to the need to have digital evidence available for a wide range of investigations or disputes e.g. patient confidentiality breaches, security incidents, criminal activities, commercial disputes, disciplinary actions and privacy issues.

These disputes present a risk to the Company's information assets, which without adequate mitigation could damage the Company's business or undermine the reputation of the Company.

Where the Company identifies a need to undertake a Forensic examination, the Company's SIRO will authorise such an assessment utilising the services of a commercial IT Forensic company.

E-mail/ Intranet/Internet

The Company and all subcontractors access NHS Mail which will be used for all correspondence and the transmission of data.

Business Continuity Plan (BCP) / Disaster Recovery Plan

The Company is obliged to have a BCP and Disaster Recovery Plan and a specific BCP is in place for the Primary Care Service.

All staff must be made aware of the relevant Business Continuity Plan and their own related roles.

The Plans will be reviewed annually.

Personal Use

A limited amount of personal use of the Company's systems is permitted subject to the following conditions:

- Only undertaken during approved breaks and not during working hours
- Personal use is in compliance with this and all other applicable Company policies/procedures e.g. email policy, internet policy, network access procedure
- Storage of personal information is clearly identified and kept to a minimum
- Staff are not permitted to transfer, store or download of any information and files for personal use including (but not limited to) MP3, AVI, WMV files and other similar formats.

Retention of Records

Records and data may be stored digitally or in paper format. In all cases the legal requirements for the retention of records will be met. These are summarised below.

(a) Records not related to employment

Subject Area	Period of Retention	Comments
Buildings and Premises – general maintenance records	3 years	
Cash Books	6 years	The Limitation Act, 1980
CCTV Images	31 days	Unless retention otherwise justified
Clinical Audit records	5 years	
Clinical System patient records	Permanent	Retain indefinitely for the foreseeable future
Complaints	10 years	Where litigation has been commenced, keep as advised by legal representatives
Contracts	6 years	The Limitation Act, 1980
Death Certificates and death Records	2 years	
Diaries (office)	1 year	
Equipment maintenance records	3 years	
Electrical Testing records	3 years	
Fire safety Records	5 years	
Freedom of Information Act Requests	3 years	
Fridge Temperature Records	1 year	
Funding data	6 years	
Insurance certificates	40 years	
Job advertisements	1 year	
Job applications and descriptions (following termination of employment)	3 years	
Medical gas storage, transport and safety	3 years	

Subject Area	Period of Retention	Comments
Minutes of Meetings	1 year	
Out of Hours Records	3 years	Where these are held as part of the clinical system the longer period of retention relating to clinical system records applies.
Paper Patient Records	20 years	20 years after last recording. 10 years after death. For patients treated under the Mental Health Act retain for 30 years after last recording.
Payroll / PAYE records	10 years	For superannuation purposes authorities may wish to retain such records until the subject reaches benefit age. Retain for 10 years after termination of employment
Personnel files (e.g. Personal files, letters of appointment, contracts references & related correspondence)	6 years	For current staff: See list in employment table. For former staff, keep for 6 years after subject of file leaves service, or until subject's 70th birthday, whichever is the later. Only the summary needs to be kept to age 70; remainder of file can be destroyed 6 years after subject leaves service.
Policies and Procedures (general operating policies)	3 years	Current version and all previous versions to be retained for a minimum 3 year period. 5 years recommended.
Purchasing orders excluding medical devices and medical equipment	18 months	
Purchasing orders - medical devices and medical equipment	11 years	
Risk assessments	3 years	Retain three years and ensure that subsequent risk assessments are available
Rotas and staff duty rosters	4 years	4 complete years following the year to which they relate
Significant Event records	3 years	Including those to be notified to the CQC
Superannuation Forms (SD55)	10 years	
VAT Records	6 years	Complete years following the end of a VAT period
Water Safety records	5 years	

(b) Employment Records Retention Periods

National minimum wage
Record: Records sufficient to establish that every worker is being, or has been, remunerated at a rate at least equal to the national minimum wage. **Retention period:** Three years from the day the pay reference period immediately following that to which the records relate ends. **Form of record:** Records must be in a form that enables the information kept about a worker in respect of a pay reference period to be produced in a single document. **Legislation:** National Minimum Wage Regulations 2015 (SI 2015/621), reg.59.
Working time restrictions
Record: Records that are adequate to show that the limits on weekly working time, daily and weekly working time for young workers, and night work (including night work involving special hazards or heavy physical or mental strain); the restriction on employing young workers during the "restricted period"; and the requirement to give every worker an opportunity of a free health assessment before he or she is transferred from day work to night work and at regular intervals thereafter are being met. **Retention period:** Two years from the date on which the records were made. **Form of record:** None prescribed. **Legislation:** Working Time Regulations 1998 (SI 1998/1833), reg.9.
Incapacity for work and statutory sick pay
Record: ● all sickness periods lasting at least four days; ● statutory sick pay (SSP) payments; and ● weeks SSP not paid and why. **Retention period:** Three years after the end of the tax year in which the sickness periods occurred and SSP payments were made. **Form of record:** None prescribed. An approved form is available from HM Revenue and Customs (SSP2 SSP record sheet) (on the HMRC website). **Legislation:** Not a statutory requirement, but HM Revenue and Customs may check that employers are paying SSP correctly and has the power to impose penalties for a failure to keep records.

Absence during pregnancy and statutory maternity pay

Record:

- the date of an employee's first day of absence from work wholly or partly because of pregnancy or confinement as notified by her and, if different, the date of the first day when such absence commenced;
- the weeks in that tax year in which statutory maternity pay (SMP) was paid to that employee and the amount paid in each week;
- any week in that tax year within the employee's maternity pay period for which no payment of SMP was made (and why); and
- any medical certificate or other evidence relating to the employee's expected week of confinement or, as appropriate, her confinement.

Retention period: Three years after the end of the tax year in which the employee's maternity pay period ended.

Form of record: None prescribed. An approved form is available from HM Revenue and Customs (SMP2 SMP record sheet) (on the HMRC website).

Legislation: Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), reg.26.

Note: Where an employer returns a medical certificate to an employee for the purpose of enabling her to make a claim for benefit, it will be sufficient for a copy of that certificate to be retained.

An employer shall not retain any certificate of birth provided as evidence of confinement by a woman who is or was an employee, but shall retain a record of the date of birth.

Statutory paternity pay, statutory shared parental pay and statutory adoption pay

Record:

- the date the paternity pay period, shared parental pay period or adoption pay period began;
- the evidence provided by the employee in support of his or her entitlement to statutory paternity pay (SPP), statutory shared parental pay (ShPP) or statutory adoption pay (SAP) (in compliance with the Statutory Paternity Pay and Statutory Adoption Pay (General) Regulations 2002 (SI 2002/2822), regs.9, 15 and 24, or statutory shared parental pay (ShPP) (in compliance with the Statutory Shared Parental Pay (General) Regulations 2014 (SI 2014/3051) regs.6, 7, 19 and 20);
- the weeks in that tax year in which payments of SPP, ShPP or SAP were made and the amount paid in each week; and

- any week in that tax year which was within the employee's paternity pay period, shared parental pay period or adoption pay period but for which no payment was made (and why).

Retention period: Three years after the end of the tax year in which payments of SPP, ShPP or SAP were made.

Form of record: None prescribed. Approved forms are available from HM Revenue and Customs SAP2 SAP record sheet, SPP2 SPP record sheet (on the HMRC website).

Legislation: Statutory Paternity Pay and Statutory Adoption Pay (Administration) Regulations 2002 (SI 2002/2820), reg.9 and Statutory Shared Parental Pay (Administration) Regulations 2014 (SI 2014/2929), reg.9

Accidents at work and work-related illness

Record: Every employer with 10 or more employees must keep readily accessible a means by which an employee may record the particulars of any accident causing personal injury to him or her.

Retention period: Minimum of three years from the date on which the record was made.

Form of record: Form BI 510 (available from the HSE books website) or an equivalent record (written or electronic) which includes the prescribed particulars, as set out in sch.4 to the Regulations.

Legislation: Social Security (Claims and Payments) Regulations 1979 (SI 1979/628), reg.25.

Injuries, fatalities, diseases and dangerous occurrences

Record: Record of any: reportable incident under regs.4-7 of the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (SI 2013/1471); reportable diagnosis under regs.8-10 of the Regulations; injury to a person at work resulting from an accident arising out of or in connection with that work, incapacitating him or her for routine work for more than three consecutive days; and other particulars approved by the Health and Safety Executive or the Office of Rail Regulation for demonstrating compliance with the approved manner of reporting under part 1 of sch.1.

Retention period: Minimum of three years from the date on which the record was made.

Form of record: None prescribed. The particulars required to be kept are set out in part 2 of sch.1 to the Regulations. Alternatively, approved forms are available from the incident reporting page on the Health and Safety Executive website, including

F2508IE - Report of an injury, F2508DOE - Report of a dangerous occurrence and F2508AE - Report of an occupational disease).

Legislation: Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (SI 2013/1471), reg.12.

Risk assessments

Record: Where an employer employs five or more employees, it shall record:

the significant findings of the risk assessment (as prescribed by the Management of Health and Safety at Work Regulations 1999, reg.3(1));

a. any group of employees identified by the risk assessment as being especially at risk; and

a. any arrangements for the effective planning, organisation, control, monitoring and review of preventive and protective measures, made in accordance with reg.5(1).

Retention period: No time limit specified.

Form of record: None prescribed. For guidance on carrying out a risk assessment see INDG163 (Five steps to risk assessment) (PDF format, 114K) (on the HSE website).

Legislation: Management of Health and Safety at Work Regulations 1999 (SI 1999/3242), regs.3 (6) and 5.

Note: The employer must review the risk assessment if there is reason to suspect that it is no longer valid or there has been a significant change in the matters to which it relates.

Exposure to specified hazardous substances

Record: Record of health surveillance, containing particulars approved by the Health and Safety Executive (HSE), of persons where appropriate (see the Control of Substances Hazardous to Health Regulations 2002, reg.11 (2)) who are, or are liable to be, exposed to substances hazardous to health.

Retention period: 40 years from the date of the last entry made in it.

Form of record: None prescribed, but must contain the information specified in Control of substances hazardous to health: Approved Code of Practice and guidance (fifth edition) (PDF format, 919K) (on the HSE website).

Legislation: Control of Substances Hazardous to Health Regulations 2002 (SI 2002/2677), reg.11.

Wages and deductions
Record: PAYE records that employers are not otherwise required to send to HM Revenue and Customs under the Income Tax (Pay As You Earn) Regulations 2003. Employers should keep full and accurate payroll records for each employee, including name; address; payslips (or other record showing gross earnings, tax, national insurance contributions and student loan deductions, and net pay); and records used to complete P11Ds. HM Revenue and Customs can ask for evidence of calculations and supporting information. **Retention period:** Three years after the end of the income tax year to which the records relate. **Form of record:** None prescribed. **Legislation:** Income Tax (Pay As You Earn) Regulations 2003 (SI 2003/2682), reg.97.

Monitoring

The Company will develop and review its information security risk management programme on a regular basis to ensure its completeness, effectiveness and relevance.

Where an incident occurs either through an audit or monitoring, the Chief Executive will review this policy and amend where applicable.

A number of regulatory bodies have responsibility for monitoring the performance of NHS organisations in relation to information security. The key regulator is the Information Commissioner, regulator of the Data Protection Act 1998 and Freedom of Information Act 2000.

Where an organisation fails to meet its obligation under the Data Protection Act 1998, Principle 7, the Information Commissioner has the power to place an enforcement notice on an organisation. The Enforcement Notice will place a legal obligation on the Company to improve its security arrangements to a level that ensures and complies with the Data Protection Act 1998.

The powers of the Information Commissioner are being increased, which will provide the Information Commissioner with the potential to be able to spot check an organisation's compliance with the Data Protection Act 1998.

References & Related Guidance

- Department of Health Confidentiality Code of Practice 2003
- Department of Health Records Management Code of Practice 2006
- Department of Health Information Security Code of Practice 2007
- Department of Health Caldicott Manual 2006
- BS ISO/IEC 17799:2005 and BS ISO/IEC 27001: 2005 & BS7799-2: 2005
- Data Protection Act 1998
- Human Rights Act 1009

- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Copyright, Designs and Patents Act 1988
- Regulatory of Investigatory Powers Act 2000
- Connecting for Health Information Governance Toolkit
- The NHS Care Records Guarantee 2006
- The NHS IM&T Operating Framework