

JOB DESCRIPTION

Job Title: Deputy Head of Information Governance & Deputy Data Protection Officer

Reporting To: Head of Information Governance and Security & DPO

Department(s)/Location: Information Governance and Security Department/
Travel to all NHS 24 sites

Job Reference number (coded):

1. JOB PURPOSE

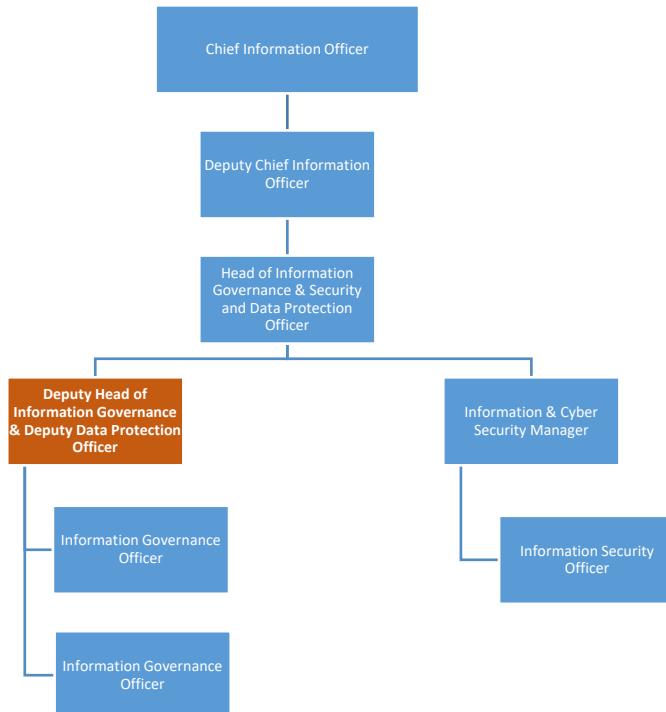
The post holder will have lead responsibility for providing leadership, support, training, guidance and effective management of all aspects of the Data Protection Act 2018 and the UK General Data Protection Regulations and Public Records (Scotland) Act 2011, Caldicott Principles, the Freedom of Information (Scotland) Act 2002 and associated relevant and supporting legislation and guidance across NHS 24.

This post is an NHS 24 wide post with an operational and legislative responsibility across the whole organisation. The Deputy Data Protection Officer (DDPO), as a subject matter expert (SME) will be a key contributor to the development of the System Security Policies for all systems processing personal data. The Deputy DPO will ensure that the organisation complies with all relevant privacy-related legislation; and that all employees are fully informed of their own responsibilities for acting within the law; and the public, are informed of their data protection rights.

The Deputy DPO will ensure that the organisation has established risk-based systems of control over the personal data that it processes and deals promptly and professionally with requests for information.

The post holder will lead in researching, developing and advising senior management on all Data Protection and Records Management requirements to ensure NHS 24 are being compliant in meeting standards.

2. ORGANISATIONAL POSITION



3. SCOPE & RANGE

NHS 24 provides the population of Scotland with access to clinical assessment, healthcare advice and information and aims to ensure that those contacting NHS 24 are given the assistance and advice they require in order to meet their health needs via the omni channel access. NHS 24 mental health services receive calls 24 hours a day and 7 days a week.

NHS 24 provides telehealth and telecare services to the people of Scotland. The Board employs approximately 1,600 staff (heads) across its six regional contact centres and six local contact centres throughout Scotland.

The function of the Information Governance & Security department within NHS 24 is to deliver and support information governance and security across the organisation.

The Information Governance and Security Department:

- Provides leadership in Records Management
- Provides the interface to the legislative competent authorities such as the UK Information Commissioner, the Scottish Information Commissioner, the Scottish Government Health Competent Authority, and the National Records of Scotland
- Ensures that all obligations under the Data Protection, Freedom of Information, Records Management and Information Security legislation are met.
- Develops and delivers training and guidance on all aspects of data protection, information security, freedom of information and records management across the organisation.
- Ensures that NHS 24 protects the confidentiality, integrity and availability of staff, patient and service user information and enables appropriate information sharing.
- Establishes relationships with other Health Boards and partner organisations in relation to the data protection, information security and records management legislation relevant to NHS 24
- Delivers the Information Governance and Security objectives within the NHS 24 Programme of Work on behalf of the NHS 24 Executive Team

The post holder has line management responsibilities and will act as an authorised signatory for signing-off of expenses for the Information Governance Administrator posts within the department. Staffing may increase as the service progresses.

This post holder will deputise on behalf of the Head of Information Governance & Security & Data Protection Officer as and when required and will attend local and/or national meetings representing NHS 24. The post holder will report directly to senior management and the Board of NHS 24 during the absence of the Head of IG & S & DPO.

4. MAIN DUTIES/RESPONSIBILITIES

This post is a key leadership role in support of the Data Protection Officer for NHS 24 which is a statutory role as defined by the UK General Data Protection Regulations and the Data Protection Act 2018. The key result areas include:

Policy Development and implementation

- The post holder will be required to lead on the assurance, compliance and advisory function on data protection legislation, records management and associated matters. The post holder will have in-depth experience and understanding of risk management and risk assessments and will have an understanding of how to respond to data breaches.
- The post holder will lead in the development of plans, systems and policies that will be disseminated into advice and guidance to all managers, staff, partner agencies and the general public thus ensuring that they are fully aware of their responsibilities and

compliance with data protection, freedom of information and records management legislation and NHS 24 policies.

Act as the specialist data protection advisor to all staff, service managers and other partners in relation to complex data requests, providing guidance and interpretation on all aspects of Data Protection, including policy implementation and development and first line support.

- Leads on the review of and providing specialist advice on highly complex Data Protection Impact Assessments and works with the Information Asset Owners to agree appropriate mitigating controls.
- Acts as the contact point for the Information Commissioners Office (ICO) on data protection issues when a Data Protection Impact Assessment has identified a high risk in the processing of personal data as required under Article 36 (Prior Consultation) of the UK General Data Protection Regulations (UK GDPR). The post holder will consult, where appropriate, with the ICO regarding any other data protection matter.
- Is the organisational lead on informing and advising the controller, partners and employees on their data protection obligations pursuant to UK GDPR and other data protection provisions (e.g., the NHS Scotland Information Governance Policy Framework). Provide specialist advice where requested in relation to the data protection impact assessment and monitor its performance (UK GDPR Article. 35).
- Is the organisational lead in monitoring compliance against the data protection regulations and associated legislation, the assignment of responsibilities, awareness-raising and specialist training of staff involved in processing operations, and the related audits.
- Works in collaboration with the Information Security Officer on the management and investigation of all reported data protection incidents and where required manage information governance and security enquiries, incidents and risks.
- Is responsible, in association with the Information Security Officer for the design and implementation of effective Data Protection and Information Governance and Security policies, processes and frameworks pan-NHS wide, including information pathways (routes to access data, including research purposes).
- The post holder will be required to interpret, complex legislation, in particular UK GDPR, the Data Protection Act 2018 (DPA) and associated updates and amendments the Public Records (Scotland) Act 2011 (PRSA), the Freedom of Information (Scotland) Act 2002 (FOISA) along with other relevant guidance from the Scottish Government, NHS Scotland, the Information Commissioners Office, the Scottish Information Commissioner, the Keeper of the Records of Scotland, multi-agency partners, contractors and other relevant parties.
- Provide advice on and apply the Exemption Clauses of the DPA and UK GDPR and provide adequate explanations to the applicant of why Exemption Clauses may have been used and ensure absolute compliance with the legislation.
- Liaise with Directors and Heads of Service to advise, embed and develop data protection, integrity and confidentiality of information within the culture of the organisation so that staff are aware of their own obligations, and those of NHS 24, under the legislation.
- Support service departments in negotiating with partners' safe, fair and lawful information sharing agreements and underpinning work instructions across partnerships and with data processors (sub-contractors).
- The post holder will be required to liaise with senior management, in particular, key roles such as the Senior Information Risk Owner (SIRO), the Caldicott Guardian and the Director of Nursing and Care. They will be required to represent the organisation when interacting with the regulators, the Information Commissioners Office (ICO), the Scottish Information Commissioner (OSIC) the Scottish Government Health Competent Authority (HealthCA), the National Records of Scotland (NRS) and will be available to address enquiries from the ICO, OSIC, HealthCA, NRS and members of the public in compliance with the requirements of the UK GDPR, DPA 2018, FOISA 2002, PRSA 2011 and NIS(R) 2018.

Training

- The post holder is responsible for Information Governance and Data Protection training within NHS 24 including the development and implementation of the training programme which will

- include establishing the training method and allow for ongoing reviews of the materials to ensure they are reflective of any new or changes to legislation.
- Develop Information Governance and Data Protection training materials that are evidence based standard and contextualised to the NHS 24 telehealth/telecare setting.

Line Management

- The post holder will have overall management responsibility for the recruitment, training, objective setting and disciplinary procedures for Information Governance and Security administrator/analyst staff and will manage all staff appraisals, personal development plans, attendance management and return to work interviews for all direct reports.
- To manage, motivate and develop Information Governance and Security administrator/analyst staff to ensure that they are able to deliver their responsibilities.
- The post holder will set objectives in line with corporate goals and actions plans to develop their team members appropriately, ensuring that all associated personal development and attendance plans and activities are completed with the required timescales.

Financial Management

- The post-holder is responsible as an authorised signatory of staff timesheets and staff expenses as per national policy, accurately entering onto the SSTS, payroll system and authorising unsociable and extra hours payments.
- Provide expert input to all NHS 24 Procurements to establish NHS 24 information governance requirements and carry out supplier evaluation and selection.

Risk and Change Management

- Responsible for assessing highly complex technical information and situations requiring analysis, interpretation and comparison of a range of options prior to approving change or mitigating a risk successfully.
- Providing expert advice on operational change
- Assessing data protection impact assessments and system security policy documents in relation to changes to all NHS 24 systems from an information governance and security perspective.
- Progressing information governance and security requirements and issues with NHS 24 and directly with suppliers and customer organisations.
- Ensure that all system design is compliant with the principles of data protection by design and by default and the security of processing.

Project Management

Provide expert input to all NHS 24 projects:

- To identify, manage and establish appropriate mitigation in respect of information risk.
- Responsible for assessing design and solution options to determine how NHS 24 information governance and security requirements are best met.

Analysis, Evaluation, Reporting and Problem Solving

- Produce reports and specifications from complex technical data suitable for a non-technical audience.
- Use experience and analytical techniques in problem solving in situations with complex facts, situations requiring analysis, interpretation and evaluation against a range of options.
- Take decisions to ensure the continuing confidentiality, integrity and availability of NHS 24 information assets.
- Produce Board and Executive Team papers outlining options and recommendations for approval.

Information Processing and Systems

- Develop and maintain systems for recording requests for information, and other associated information such as Requirements for Reviews by the Board's Data Protection Officer and ensure data quality and consistency.
- Responsible for the management of the Information Asset Register, the Record of Processing Activities and the Information Risk Register on behalf of the DPO and the SIRO. Co-ordinate, review and provide advice on data protection impact assessments and/or information assets risk assessments on behalf of the Head of IG & S & DPO and SIRO.
- Organise and manage papers for the Board's Information Governance & Security Group. This includes providing regular performance monitoring reports on the Board's performance against legislative timescales and updating the group on current national development in UK GDPR/DPA and Records Management and related legislation.

5. SYSTEMS & EQUIPMENT

General Equipment – Use of personal computer or laptop, telephone, multi-function device and audio-visual equipment. The post holder will, on a daily basis, be required to use standard software packages [Microsoft Office], e-mail, the internet, and NHS 24's intranet, in carrying out the main duties and responsibilities associated with this post.

Specific Systems included in the Microsoft Office 365 suite such as:

- Microsoft Word: For general day-to-day use including report, planning and copywriting.
- Microsoft Excel: To create, store and produce data for report generation & record keeping.
- Microsoft PowerPoint: For producing presentations to update stakeholders.
- Microsoft Outlook: For effective and efficient communication with everyone in the organisation and external stakeholders as well as diary management.
- SharePoint: Resource and project planning.
- MetaCompliance: For providing communications and policies to staff.

Responsible for the development and maintenance of systems such as the Information Asset Register, Information Risk Registers, Data Protection Impact Assessment systems, Record of Processing etc.

Microsoft Visio – to create and maintain design models requiring extensive concentrated effort and keyboard skills to support enterprise modelling.

Further to NHS 24 having invested in a revolutionary technology change allowing the enrichment of our existing services and providing a platform to achieve service agility and greater empowerment for our business than we have seen before. This will support our strategic intent to help us mobilise future initiatives quickly, at lower cost and efficiency and ultimately provide a better service at lower cost to the Scottish public.

A high-level summary of the technology environment used to implement this capability is:

- SAP CC - A multi-channel technology platform that will support our current and future strategic objectives to reach out to our patient community in a variety of existing and emerging communication methods (largely focussed on telephony).
- SAP CRM - A packaged core I.T. solution to support our patient relationship management requirements which includes workflow, call management and campaign execution functionality.
- Infermed/Arezzo - An integrated clinical decision support tool that will enable NHS24 to create, change and publish content in an agile manner.
- Open Text - A knowledge management system that will provide key capabilities to author and publish documents and other knowledge artefacts to make available the right knowledge at the right time.
- SAP BI/BO - A leading reporting solution that underpins and informs key operational and management KPI data. This will be made available using the principles of the timeliness so we

can quickly identify emerging trends or patient behaviours and therefore manage our services in a pro-active way; and

- SAP PI - An integration platform that will support data and process exchange between our existing applications and systems.

6. DECISIONS & JUDGEMENTS

The post holder is directly accountable to the Head of Information Governance, Security and Data Protection Officer for the leadership and management of Data Protection and Information Governance work and strategic objectives.

Performance objectives are agreed annually with the Head of Information Governance, Security and Data Protection Officer.

The post holder works autonomously and is required to exercise a high level of initiative, judgement and discretion in deciding what personal information to release to applicants, including requests from Police Scotland, considering data protection exemption categories, requiring an expert understanding of the UK GDPR/Data Protection legislation, the ability to accurately interpret complex legislation and the ability to convince the Chief Executive, Directors and members of the senior management team in relation to the disclosure of information.

The post holder will provide expert knowledge and advice across the whole organisation. The post is expected to function as a source of expertise and advice at the highest levels, with the freedom to act on behalf of NHS 24 in relation to external and internal issues. The post-holder is expected to use their own initiative in making decisions when prioritising their own and the team's deadlines and workloads.

In the absence of the Head of Information Governance, Security and Data Protection Officer, to the highest level of management in the organisation (or group of undertakings) via the Deputy Chief Information Officer and/or the Senior Information Risk Owner.

Sound judgement, flexibility and the ability to maintain performance under consistent pressure of short timescales are essential in the performance of duties.

The post holder is accountable for leading and driving progress in identified areas of responsibility.

The post holder will be a lead contributor to the development of the information governance strategy for the organisation, formulating and adjusting the relevant organisation wide policies, processes and procedures to ensure compliance with this strategy.

The post holder will work with the L&PE department to develop, implement, asses and adjust both online and face to face training plans, packages and sessions across the full range of their legislative portfolio to ensure that the training and education of all staff, including senior staff such as Head of Service and Information Asset Owners is compliant with the latest requirements of the legislation.

The post holder will work with other senior Information Governance staff from partner Health Boards to establish and implement Once for Scotland training packages to ensure a common level of across NHS Scotland.

7. COMMUNICATIONS & RELATIONSHIPS

The post holder will require excellent communication, facilitation and negotiation skills as there will be a continual requirement for the post holder to communicate regularly with wide range of senior clinical and non-clinical staff across NHS 24, professional and partner organisations patient, public and staff at all levels.

JOB DESCRIPTION

The post holder will be required to write reports interpreting and explaining highly complex legislation to allow full understanding. It will also require the post holder to present to the Board Standing Committees and provide appropriate training to the Information Asset Owners and Committee Members.

The post holder will deal with and be required to deliver contentious and highly complex and confidential information in a sensitive manner, showing tact and understanding.

The post holder will be responsible for negotiating with peers and information governance staff from other health boards and reconciling the differing opinions to the benefit of NHS 24.

The post holder will be required to use their interpersonal and communication skills to overcome significant barriers when communicating in a hostile and highly emotive environment, explaining complex legislative requirements to data subjects and their representatives.

Devise and deliver formal and informal information governance and data protection training, across NHS 24.

The post holder will deal directly with members of the public in what may be highly emotional circumstances providing advice on data protection matters such as highly contentious data subject access requests.

The following are key working relationships involving regular contact:

Internal

- Senior Information Risk Owner
- Caldicott Guardian
- Deputy Chief Information Officer
- NHS 24 Executive Team and Board to report on and explain information governance and security reports.
- NHS 24 Senior Management Team in relation to information governance and security and records management requirements.
- Programme Management team to discuss the data protection and information security implications and requirements on their programmes of work.
- Staff within NHS 24.

External

- Information Commissioners Office.
- Scottish Information Commissioner.
- National Records of Scotland.
- Scottish Government Health Competent Authority.
- NHS Scotland Information Governance Forum.
- NHS Scotland Data Protection Officer Forum
- NHS Scotland Records Management Forum.
- NHS Scotland Freedom of Information Forum.
- Information Governance and Information Security leads in other NHS Boards.
- Members of the public.
- Any individual or organisation who submits a request for information to NHS 24.

8. PHYSICAL DEMANDS OF THE JOB

Mental:

- Frequent concentration required for production of responses to requests for information often to meet tight deadlines. High levels of concentration required for responses where complex arguments may be developed, for example in compiling submissions to appeal investigations.
- High levels of concentration required when attending meetings.

- Unpredictable work pattern with changing and competing priorities,
- Keeping up to date with the evolving nature of data protection legislation and other information rights legislation.
- Retention and communication of knowledge and information.
- Need to communicate clearly and persuasively with staff at all levels, public, patients (as data subjects who may wish to exercise their data protection rights) and other external contacts.
- Work takes place in an open plan environment where there are frequent interruptions from telephone calls, managers' requests, office noise and visitors.
- There may be times when both the post holder and their direct reports will work from home in a solitary fashion and they must be aware of the mental health aspects of this, both for themselves and their direct reports.

Emotional:

- The resilience to cope with difficult and demanding members of the public, some of whom will inundate the organisation with frequent and multiple data protection and information rights legislation requests which can include those of a frivolous and vexatious nature.
- The ability to meet tight deadlines and maintain high standards of work whilst dealing with persistent interruptions, resulting in the constant reprioritisation of work.
- Mental endurance to cope with the many and varied aspects of the post and the need to be able to respond to new developments in data protection practice where there is little or no previous guidance.
- Emotional resilience in making requests direct to Directors/Senior Managers and convincing and influencing them to provide the information required by the deadline. This includes reiterating or escalating these requests if no response received.
- Constant pressure of always working to statutory deadlines in order to comply with legal requirements.
- As a line manager there may be exposure to highly distressing or emotional circumstances:
 - Dealing with staff interpersonal and disciplinary issues.
 - Dealing with staff and managers who are under stress both in development interventions and in meetings.
 - Supporting staff/manager whilst undergoing organisational change.

Working Conditions:

- Use of computer equipment for the majority of the working day for word processing, email, internet research and data input, resulting in frequent sitting in a restricted position, prolonged typing and use of VDU screen.
- Occasional travel to various sites across the NHS 24 estate and beyond to national meetings and events.

9. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

Regular negotiation with Directors/Senior Managers particularly when faced with resistance or reluctance. The post-holder may be required to personally challenge standards and/or practice that may compromise or be detrimental to NHS 24's compliance obligations.

Convincing Directors and Senior Managers across NHS 24 of the requirements of data protection legislation and the need to share/provide information, especially when they are reluctant to share this. Ensure staff across the organisation take information requests seriously.

Work with external organisations e.g., contractors to ensure appropriate use of the exemption clauses of the relevant Act and protect the reputation of the organisation.

Deal with the complexities and requirements of meeting the needs of different information rights legislation and the interface between them, i.e. UK General Data Protection Regulations, Data Protection Act 2018, Freedom of Information (Scotland) Act 2002, Public Records (Scotland) Act 2011, The Network and Information Systems Regulations 2018, Access to Health Records Act 1990 and the duty of confidentiality regarding patient confidentiality issues.

Dealing with frivolous and vexatious individuals who make multiple requests for information.

Exposure to information which can be distressing around individual cases.

Frequent liaison with the Information Commissioner's Office and staff on complex cases and data breach investigations.

The post holder must be able to prioritise a busy workload where there will be competing demands. This will involve the successful delivery of local and national targets as well as meeting the expectations of individual members of the public.

The post holder is expected to provide professional leadership and training to the IG&S team.

10. KNOWLEDGE, TRAINING & EXPERIENCE REQUIRED TO DO THE JOB

Education

- Be educated to a master's level equivalent qualification/professional qualification or able to demonstrate an equivalent experience in data protection and information governance.
- Ideally hold or be prepared to work towards a qualification in Healthcare Information Governance, along with Data Protection certifications such as UK GDPR practitioner or IAPP CIPP/E.

Experience:

- Expert knowledge of the Data Protection Act, 2018, the UK General Data Protection Regulations and the Public Records (Scotland) Act and other related legislation including the Caldicott principles.
- Extensive experience working in an organisation interpreting complex data protection and information handling requirements.
- Experience working in an information governance or similar data protection role.
- Significant experience in a Business Analysis role.
- Demonstrable experience in the production and presentation of information for Senior Management including co-ordination and organisation of large committee meetings.
- Proven ability to prepare and present complex material to a mixed audience.
- Experience in developing and maintaining Data Protection policy, processes and procedures.
- Proven track record in advising/training staff.
- Knowledge of information technology, information assurance, legislation and records management (both manual and electronic).

Skills:

- A decision maker with demonstrable ability to act independently and use own initiative.
- Excellent Communicator with a friendly and professional approach.
- Excellent analytical skills with an understanding of information governance, security and records management issues.
- Excellent Facilitation and presentation skills.
- Leadership and team working skills, highly motivated, assertive and confident.

11. JOB DESCRIPTION AGREEMENT

A separate job description will need to be signed off by each jobholder to whom the job description applies.

Job Holder's Signature:

Date:

Head of Department Signature:

Date:

JOB DESCRIPTION



--	--