JOB DESCRIPTION

Job Title: **Head of Information Governance & Security & Data Protection Officer**

Reporting To: **Deputy Chief Information Officer**

Department(s)/Location: **Information Governance and Security**

Job Reference number (coded):

1. JOB PURPOSE

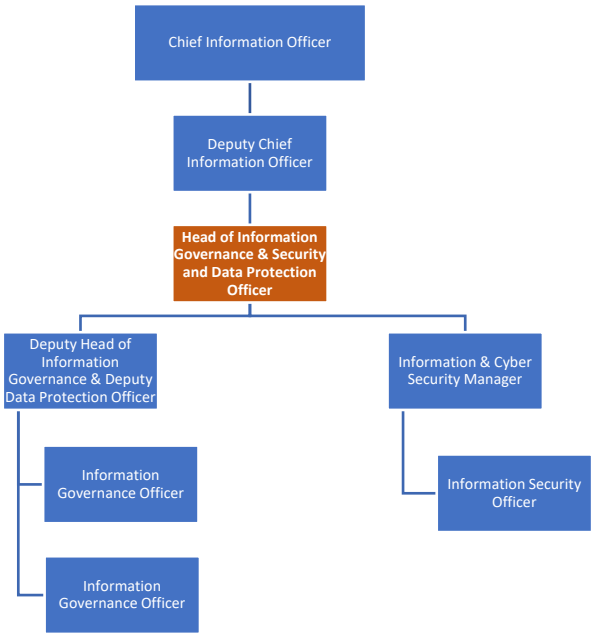
Provide strategic leadership for Information Governance and Security across NHS 24, providing assurance to the Board regarding the performance of NHS 24 in line with governance and accountability requirements.

Produce the NHS 24 Information Governance and Security Strategy, objectives and work plan to ensure that key functions are managed and progressed as appropriate which includes the confidentiality and safety of patient and staff information.

Ensure the overarching principles of Information Governance and Security are embedded in the organisation, setting targets against indicators to ensure these are applied across NHS 24 and therefore deal with difficult issues on a daily basis.

Take a lead management role for the ongoing teaching / training of all staff across the Board area relating to Information Governance, Data Protection, Information Security and associated Risk Register entries and Records Management to ensure that they are aware of their personal responsibility in relation to the use, storage and sharing of information.

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.

The Information Security & Governance function is responsible for ensuring the organisation is compliant with all legal and regulatory requirements for information. This includes all forms of information in all formats i.e electronic files, published data, records, paper based information. This function is also responsible for the physical security of the organisations estate.

The post holder will:

- Lead and manage the Information Governance and Security team, delegating work, conducting Personal Development Planning Reviews, managing absence, capability, competence, and taking forward investigations as necessary to the situation

- Manage the Information Governance and Security budget and other additional budgets for projects as required.

The post holder has lead responsibility as the organisation's 'Accountable Data Protection Officer' as required by the General Data Protection Regulations (GDPR) to ensure the Board is legislatively compliant regarding the information held.

Take lead responsibility as the organisations security officer in relation to all aspects of physical security for all NHS 24 premises.

As the 'Lead Responsible Officer' on behalf of the Board, liaising with Police Scotland, The Centre for the Protection of National Infrastructure and other government agencies as required, implement necessary actions to ensure the physical security of all NHS 24 locations and the safety of all NHS 24 staff.

4. MAIN DUTIES/RESPONSIBILITIES

Patient Client Care

The post holder is responsible for meeting directly with patients and family members to discuss issues relating to how their personal and / or clinical information has been handled or shared, providing advice and guidance relating to the Board's legal obligations, policy processes and procedures and timescales for outcomes.

Meet with members of staff who have direct patient / client caring responsibilities, providing advice and guidance on the use, security and confidentiality of the information they are handling on a daily basis to ensure that this is dealt with appropriately and not shared in a manner that will cause offence.

Strategic Focus

Provide strategic leadership for Information Governance and Security across NHS 24, providing assurance to the Board regarding the performance of NHS 24 in line with Information Governance and Security and accountability structures.

Produce the NHS 24 Information Governance and Security Strategy that contains objectives and a work plan to ensure that the responsibilities of the department are taken forward and completed as required.

Ensure clear links to the overall NHS 24 strategic priorities in Information Governance and Security in line with national and local strategies.

Lead projects relating to decommissioning work when the reorganisation of services takes place, advising the Board of appropriate actions required to be taken.

Direct and lead the development of corporate Information Governance and Security objectives, integrating corporate objectives and strategic priorities into a framework. To work with key Workforce stakeholders to ensure that Information Governance and Security is part of personal development for all staff in NHS 24.

Direct the Information Governance and Security Improvement Framework across NHS 24, ensuring that corporate objectives and strategic priorities are integrated and system wide monitoring, assessment and management arrangements are in place throughout the organisation.

Direct the physical security improvement framework across NHS 24, ensuring that corporate objectives regarding staff safety and location security are embedded in to day-to-day procedures and processes, setting targets and indicators to ensure delivery.

Policy and Service Development

Influence Scottish Government policy and strategy developments in relation to Information Governance and Security. The post holder will be responsible for interpretation and implementation of national policies across NHS 24.

Accountable for the development and implementation of NHS 24 policies in relation to Information Governance and Security across the organisation. This includes policies for physical access to buildings, access to systems, access to data (electronic or paper based), FOI request access, internet access, mobile phone usage as an example.

Direct the Information Governance improvement framework within NHS 24, ensuring that system wide monitoring, assessment and management arrangements are in place throughout the organisation.

Ensure a transparent approach to the management of Information Governance and Security across NHS 24 with explicit links to strategy development, operational delivery of services and clarity of reporting mechanisms at all levels.

Lead specific pieces of work, in partnership with the Senior Officials within Partner Agencies and Health, to develop where appropriate joint working in Information Governance and Security, through the development and implementation of Information Sharing Protocols.

Deal with a broad range of often difficult and delicate Information Governance and Security issues that will require the interpretation of the Board's legal position, providing sound advice and guidance to assist with the resolution of these.

Deal with legal issues and cases in collaboration with the Central Legal Office that could relate to social media issues, being involved in investigations and providing evidence of activities that may result in disciplinary sanctions and possibly dismissals.

Function as the 'Lead Responsible Officer' on behalf of the Board, reporting to the Information Commissions Office, undertake investigations, and implement necessary actions that the Information Commission Office (ICO) have deemed necessary to avoid fines or enforcements that will have a negative reputational and / or financial impact on the organisation.

As the 'Lead Responsible Officer' on behalf of the Board, reporting to the Scottish Information Commissioners, undertake investigations, and implement necessary actions that the Office of the Scottish Information Commissioner (OSIC) have deemed necessary to avoid enforcement notices that will have a negative reputational impact on the organisation.

Challenge standards and practices that may be in breach of the relevant Acts, and suggest practical solutions (e.g. ICO Employment Code of Practice that has implications for Workforce) that will minimise risk to NHS 24.

Finance and Physical Resources

The post holder is responsible for the production of business cases to secure increases in the departmental budget and management thereafter.

Manage the Information Governance and Security budget including all physical security budgetary requirements and other additional budgets for projects as required. The post holder is responsible for ensuring the effective and efficient utilisation of the budget as required to meet financial requirements of the reporting staff which may include training and education.

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.

Ensure the physical safety of all NHS 24 staff and the physical security of all NHS 24 locations.

Manage the overall Information Governance and Security budget incorporating the data protection, information security, physical security, with responsibility for the physical security assets, and records management services and other additional budgets for projects as required.

Staff Management/Supervision, Human Resources, Leadership and/or Training

Lead and manage the Information Governance and Security team throughout the entire employee life cycle, including recruitment, delegating work, appraisals, managing absence, capability, competence, taking forward investigations as necessary to the situation and conducting Personal Development Planning Reviews to make sure staff are supported and confident in undertaking their roles.

Take a lead management role for the ongoing teaching / training of all staff across the Board area relating to Information Governance, Data Protection, Information Security, Risk Register entries,

Freedom of Information and Records Management to ensure that they are aware of their personal responsibility in relation to the use, storage and sharing of information.

Provide cross organisational training in Information Governance and Security to all departments, Independent Contractors, Partner Organisations, Integration Joint Boards and the general public as necessary to ensure that the relevant information is shared.

Information Systems and Reporting

Ensure on behalf of the Board that all of the data, patient and staff, clinical and non-clinical held, is monitored and managed and that the confidentiality of this information is maintained to the required standards.

Manage and develop Board wide the Records Management System (RMS), Information Asset Register (IAR), Record of Processing Activity (RoPA), Information Security Risk Register (ISRR), and Safeguard System (SS) for sharing information to ensure the confidentiality of people's health and care information as well as making sure it is used properly.

Lead on corporate reporting of Information Governance and Security matters with a requirement to be a member of each major Board group relating to the management of organisational information.

Provide technical advice and support on all aspects of information storage including technical support for correct records management.

Manage and develop information systems or equivalent e.g. Information Asset Register, Information Security Risk Register, Records Management functions which apply across the organisation.

Manage, on an ongoing basis Subject Access (SA) / Freedom of Information (FOI) requests as a major part of the role ensuring that processes are strictly followed within the relevant deadlines so that the organisation is not legally compromised.

Investigate and follow up potential breaches of data security interpreting the Data Protection Principles, Caldicott Principles and guidance from Professional bodies.

Responsible for providing information regarding Significant Adverse Events such as, child protection issues, breaches of physical security, CCTV footage, providing evidence where possible.

Ensure that a database of training records on Information governance and security is maintained by the Learning and Development department on an ongoing basis to be able to report statistics to the Board.

Ensure that information is collated, maintained as a record of notification of processing which is used for annual reporting to the Information Commissioner.

Provide reports and other papers as required, collating and manipulating data as necessary to provide a clear picture of compliance with Regulations, business cases for equipment and / or resources, reporting of incidents, advice and guidance for staff and managers, annual training statistics.

Liaise with Head of ICT to ensure the security of the Network; Major Clinical Systems such as; the Radiology System; Theatre System; Patient Administration System; Pharmacy system; Maternity system.

Liaise with the Head of ICT Operations to ensure the security of non Clinical Systems such as email (comprising the email systems in use across NHS 24) and the Intranet and internet are in compliance with data protection advising on information security as appropriate.

Research and Development

As a member of the National Operational Group and the Public Benefit Privacy Panel, be involved in decision making regarding research and development relating to redesign, audits and service improvement regarding Information Governance and Security and the implementation of post research outcomes.

Ensure on behalf of the Board that all of the data, patient and staff, clinical and non-clinical held, is monitored and managed and that the confidentiality of this information is maintained to the required standards.

Monitor and audit the information systems used including the cyber security of these across the organisation.

Ensure that Caldicott and FOI processes are followed and managed in line with the required deadlines.

As a member of the National Operational Group and the Public Benefit Privacy Panel, be involved on an ongoing basis in decision making regarding monitoring, audits and / or research and development projects relating to the redesign and service improvements in relation to Information Governance and Security and the implementation of post research outcomes.

Regular testing of security equipment, systems and potential solutions which will have an impact to Board processes delivery of services.

5. SYSTEMS & EQUIPMENT

The post holder will be expected to use the following systems and equipment:

- Building Access system (owner of the system)
- Redaction Software for FOI responses (system owner)
- CCTV for all the buildings in the organisations estate (system owner)
- Microsoft office/Office 365 including PowerPoint, excel and word
- Collaboration tools such as SharePoint, Knowledge Hub etc.
- Quality Improvement tools
- Programme/Project Management tools
- Business Objects/Google analytics for the interpretation of data
- Data and information Business Intelligence suite
- HR Management Information System for recording and managing team members' absence history and approving staff member expenses.(e.g. SSTS, eESS, eExpenses)
- The post holder will require to be proficient in the operation of a PC/Tablet/Smartphone device to access and utilise corporate systems.

6. DECISIONS & JUDGEMENTS

This post reports to the Chief Information Officer of NHS 24 and is responsible for the strategic leadership for Information Governance and Security and physical security across NHS 24, providing assurance to the Board regarding the performance of NHS 24 in line with governance and accountability requirements.

Being fully accountable for leading and driving progress within a broad sphere of legislation and standards and within the parameters of established national and local priorities, policies and procedures which are required to be interpreted there is a need to operate autonomously and function as a source of expertise and advice at a strategic level.

Responsible for interpreting and implementing national policy and guidance, advising the Executive Management Team how to achieve their statutory requirements by identifying the required change to practice for service development.

Providing corporate level leadership relating to Information Governance and Security driving the progress of ensuring that the Board is in compliance with all relevant regulations.

Perform detailed, critical technical analysis of system and database problems relating to Information Governance and Security and provide a balanced assessment of recommended actions and / or solutions.

As the lead expert for Information Governance and Security the post holder will deal with a broad range of issues that require investigation, analysing findings and making recommendations about corrective actions and / or provide sound advice and / or guidance as necessary.

Direct the development of the local work/implementation plans liaising with key managerial leads to agree targets and projections.

Ensure the appropriate strategic direction and implementation of the Information Governance and Security Strategy and direct developments of Information Governance and Security arrangements ensuring system wide review, action planning and reporting arrangements are in place as part of NHS 24 strategic and operational management assurance to the appropriate Governance Committees.

Specifically champion and support the integration of Information Governance and Security requirements in day to day operational management with the aim of improving compliance.

Where there is a need, the Chief Information Officer, Medical Director or Director of Nursing and Care will give the authority to proceed with matters out with the delegated authority or immediate role and function of the job.

With the Chief Information Officer the post holder is expected to deal with a broad range of difficult situations such as leading meetings, influencing NHS staff and managers at all levels of seniority, public speaking, analysing technical and other system problems and proposing solutions, often working under pressure and balancing multiple demands in a complex / changing environment.

Advice and guidance is available from the Chief Information Officer, the Medical Director, The Director of Nursing and Care or the relevant Regulatory bodies as necessary to the issue being managed.

Work will be review as necessary to the scope of the job. Formal Personal Development Planning and Review will take place annually when objectives will be discussed and agreed.

7. COMMUNICATIONS & RELATIONSHIPS

The post holder is required to have excellent communication and interpersonal skills, both written and verbal. Strategic thinking and the ability to anticipate and resolve problems before they arise and respond to sudden unexpected demands.

Provide detailed advice, guidance and support to Managers and Accountable Officers in their roles, regarding all aspects of Information Governance and Security in line with the associated legislation (e.g. Data Protection Act 2018, Common Law Duty of Confidence, Freedom of Information (Scotland) Act 2002) and the Public Records (Scotland) Act 2011.

Deal directly with service users and staff regarding complaints and investigations, including Serious Adverse Events that need to be dealt with in a discrete and delicate manner.

Directly influence and advise the EMT, Committees and the Board on all aspects of Information Governance and Security and with Partner agencies including the Joint Integrated Boards and GP Practices. There may communication required with very complex technical content. This needs to be communicated in a way that is understandable by those without technical expertise.

The post holder must be extremely diplomatic and show the utmost discretion in communications regarding information sharing regarding GDPR breaches, break ins, cyber attacks etc.

Deal with some particularly difficult situations including the production of Freedom of Information Act 2002 reviews, which have to be looked at from the public's perspective and the organisation's perspective which can include ethical and moral dilemmas that may cause concern.

Take part in conversations and meetings where the subject matter may be delicate and upsetting, having to direct the conversation in a way that causes the least angst in trying to reach consensus.

Interpret changes in legislation for the Board to ensure that the organisation complies with its legal responsibilities in relation to Information Governance, Data Protection, Freedom of Information, Information Security etc. and advising the public regarding these where appropriate.

Train small and large groups of staff regarding Information Governance, Data Protection, Freedom of Information, Information Security, Physical Security etc. and give presentations on a regular basis within and out with the health service including directly to the public as necessary.

Develop and maintain effective, positive relationships with key partners and partner organisations, providing a positive role model for partnership working within NHS 24.

Take part in investigatory hearings that involve potential breaches in confidentiality, sharing information inappropriately, and involvement in social media conversations relating to the Board or staff who work for the Board and other Information Governance and Security incidents.

The post holder will provide and receive highly complex, highly sensitive and, at times, highly contentious information which may involve hostile, antagonistic and highly emotive episodes.

Internal Stakeholders

- Senior Information Risk Owner
- Caldicott Guardian
- NHS 24 Executive Team and Board to report on and explain information governance and security reports
- Board Standing Committee Chairpersons and non-Executive members
- 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
- Heads Of Clinical Services
- Heads of Department
- Staff within NHS 24

External Stakeholders

- Information Commissioners Office
- Scottish Information Commissioner
- National Records of Scotland
- Scottish Government Health Competent Authority
- Relevant Scottish Government departments are required based on the legislative portfolio of the role
- NHS Scotland Information Governance Forum
- NHS Scotland Information Security Forum
- NHS Scotland Records Management Forum
- NHS Scotland Freedom of Information Forum
- Information Governance and Information Security leads in other NHS Boards
- NHS Scotland Boards Data Protection Officers
- Scottish Business Resilience Centre
- Police Scotland
- Scottish Government Cyber Resilience Centre
- NHS Scotland Central Legal Office
- Members of the public
- Any individual or organisation who submits a request for information to NHS 24
- The Centre for the Protection of National Infrastructure
- The National Cyber Security Centre

8. PHYSICAL DEMANDS OF THE JOB

Physical

Frequently lift equipment and materials such as a projector, laptop, handout material (in excess of 5Kg) for e.g. preparing and conducting presentations and staff awareness sessions.

Stand for prolonged periods up to 14 hours per month, delivering training awareness sessions to all levels of staff.

Stretch and bend to file information or to retrieve information for meetings.

Mental

Frequent prolonged concentration required to perform detailed, critical technical analysis of system and database problems relating to Information Governance and Security and provide a balanced assessment of recommended and / or solutions. Given the nature of the role the post holder will be subject to frequent interruptions.

Review internet logs as necessary that require long periods of focussed concentration and may involve viewing disturbing images that need to be gathered as evidence.

Attend formal stage policy process meetings to present findings with suspected perpetrators to present findings and provide specific Information Governance and Security legal advice and guidance.

Attend formal meetings with Police Scotland and the Centre for the Protection of National Infrastructure where all matters of physical security are reviewed and assessed.

Frequently use in-depth mental attention when leading meetings, influencing NHS staff and managers at all levels of seniority, public speaking, analysing technical and other system problems and proposing solutions, often working under pressure and balancing multiple demands in a complex / changing environment.

Emotional

Deal with situations where there is conflict and / or heated discussions, e.g., at emotionally charged meetings where a member of staff may be in breach of Regulations and give advice regarding subsequent actions that need to be put into place.

Direct line management requires emotional effort when applying Human Resource policies and procedures i.e. addressing and managing sickness, disciplinary and performance management issues. This may involve delivering or investigating uncomfortable and disputed issues.

Deal with cases where there may be a need to challenge standards and practices that may be in breach of an Act, and to suggest practical solutions (e.g. ICO Employment Code of Practice has implications for Human Resources) that will minimise risk to NHS 24.

Deal regularly with conflicting and challenging problems that require sustained emotional resilience such as when there is a need to respond immediately to questions or advice that is being sought, particularly when there has been a Severe Adverse Event.

Review internet logs as necessary that require long periods of focussed concentration and may involve viewing disturbing images that need to be gathered as evidence.

Attend formal stage policy process meetings with suspected perpetrators to present findings and provide specific Information Governance and Security legal advice and guidance.

Deal occasionally with data subjects who may present severely challenging behaviour under emotional circumstances

Working Conditions

Work with a computer for word processing, creating presentations, developing business plans and other strategic documents for consideration at Board level, using the email and inputting data into protected database and systems.

9. MOST CHALLENGING/DIFFICULT PARTS OF THE JOB

The post holder is required to have a current knowledge of changes to legislation and guidance to ensure that the organisation is compliant with all aspects of Information Governance. This will involve interpreting highly complex Information Governance legislation which will be multi-stranded and may change current legislative interpretations

To engage management and staff, supporting interest and involvement in the elements of the Data Protection Act, Freedom of Information Act and other relevant legislation, contributing to induction and other training for staff to maintain a high profile within the organisation.

Establishing, maintaining and monitoring for compliance the security scope and boundaries of all third parties and suppliers to ensure they are appropriate and fully understood and implemented by all.

Establishing, maintaining and monitoring for compliance the physical access to buildings and adherence to policy regarding identity badges.

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

Qualifications

Educated to degree level with an additional qualification at postgraduate diploma level in management.

Additional specific Masters Degree in Information Governance is essential to be able to perform to the required level and standard.

Experience

Substantial amount of experience working within the field of Information Governance and Security.

There is a requirement to have experience in the creating, developing and implementing policies, procedures, guidance and protocols.

There should be a proven track record in the provision of creative and innovative solutions in meeting organisational requirements.

Proven track record in project management

Skills

Demonstrate integrity and effective leadership and management skills together with a proven track record of achievement in strategy and policy development and implementation.

Evidence of developing and maintaining effective, positive relationships with key individuals and organisations, providing a positive role model for partnership working within NHS 24.

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:** **Head of Department Signature:**	**Date:** **Date:**