Maidstone and Tunbridge Wells NHS Trust
JOB DESCRIPTION

Job Title: Head of Information Governance & ICT Risk
                         Management

Grade: 8b

Care Group / Department: Information & Communications Technology (ICT)

Base: Maidstone Hospital

Hours: 37.5

Reports to: Director of ICT

Accountable to: Director of ICT

_____

Job Summary:

As an expert in this field the Information Governance Manager and ICT Risk Manager is responsible for the strategic and operational management of the information governance agenda across the entire Trust, bringing together Information Governance Management, Confidentiality, Data Protection, Caldicott, Records Management, Information Quality Assurance, Information Security and Freedom of Information.   The post holder will develop, integrate and implement the Trust's Information Governance and Information Risk strategies across the complex areas of clinical and corporate services, based on a sound understanding of current legislative requirements, continually changing technology advances and national requirements and continue to raise levels of knowledge and awareness across all staff as an important contributor towards high quality patient care.

To advise on and assist to develop the trusts Information Governance agenda, long and medium-term plans, general policies, procedures and guidance for the trust.

Changes to or new implementations relating to Trust systems or processes which involve the processing of personal data must have full IG assurance. The Head of Information Governance is responsible for ensuring that this is completed and for managing and recording any key associated risks.

To advise on access to and management of records and Freedom of Information requests with regard to ICT; providing, receiving and analysing complex, sensitive and sometimes highly contentious information; guiding users to the correct course of action; sometimes requiring contact with patients or external stakeholders.

To provide specialist expert advice to the Caldicott Guardian Senior Information Risk Owner (SIRO) and service leads, in making sure the trust operates within legal and ethical frameworks.

To provide advice, expert support and assurance on the implementation and delivery of plans to maintain and improve good information governance practice for the trust.

To work closely with staff across the organisation to communicate Information Governance standards and issues; developing and delivering where appropriate formal training and presentations to groups of trust staff.

To ensure the provision of a highly professional, customer-focused Information Governance and ICT Risk Management service which supports the delivery of high-quality patient care.

Liaising with other NHS and public sector organisations involved in Information Governance coordination and projects across the NHS and Social Care provision in Kent and Medway

Ensuring all ICT risks are identified, managed, recorded and tracked according to the Trust's Risk Management policies and procedures.

To deputise for the Director of ICT as required

To represent the Trust at external meetings as required

The post holder is responsible to the Director of ICT for:

- Information Governance
- Information Governance Management
- Information Security
- Information Governance Training
- BS7799 /ISO 27001/ISO 27002
- Freedom of Information
- Data Protection
- Data Quality
- Confidentiality
- IG aspects of Information Quality Assurance
- Information sharing
- Development and documentation of policies and procedures
- ICT Risk Management (both physical and cyber)

Working relationships:
- Maidstone & Tunbridge Wells Trust Board and Executive Directors
- All Divisions, Directorates and Departments
- Kent & Medway Information Governance Forum and subgroups

- NHS Digital
- NHS X
- Integrated Care System IG
- NHS Counter Fraud Service
- Information Commissioner and other statutory bodies
- Patients and Members of the public
- Risk and Incident Management Teams
- Internal / External Auditors
- Suppliers
- Regional and National Strategic Information Governance Network (SIGN) Groups

Budget Responsibilities: Budget holder for the Information Governance budget with responsibility for the day to day management of the budget. Authorised signatory for elements of the overarching ICT budget

DIMENSIONS

Information Governance
- To provide an Information Governance service to the Trust to ensure Information Governance principles are embedded in Trust's activities.

Information Governance Management
- To implement and support an Information Governance Management framework within the Trust.
- To provide advice and guidance on Information Governance and ICT risk to trust staff and to external agencies as required.
- Lead the Trust in maintaining compliance with the Data Security and Protection Toolkit, ensuring that submissions to NHS Digital are made correctly within prescribed timescales and that they are signed off by Information Governance Committee and Trust Board.

Information Governance Training
- To ensure all Trust staff receive the relevant level of Information Governance training.

Information Security
- Ensure the Trust is in compliance with all Information Security legislation and guidance, especially ISO 27001 / 27002, the Network and Information Systems Regulations and that the Trust has a Cyber Security Programme working to ensure that measures are actively in place to protect NHS assets and services, this will include completing independent assessments, ensuring that assessment outcomes are acted upon to mitigate identified risks and ensuring that the Trust is registered with NHS Digital and is responsive to Cyber alerts and advisories when they are issued.

Freedom of Information (FOI)
- To provide support and guidance to the Trust on all aspects of FOI and ensure the Trust is meeting its statutory obligations.

Data Protection

- To ensure the Trust has an Information culture that adheres to the Data Protection principles.

ICT Risk Management

- To support the Director of ICT in developing and maintaining the Trust IG and ICT Risk Management Strategy
- To ensure all ICT risks and incidents are identified and managed according to the Trust Risk Management Strategy
- Ensure that procedures for managing information security within the Trust are effective and aligned with the Trust's overall risk approach.

Documentation

- To ensure all policies and procedures related to IG and ICT Risk Management are in place and updated as required.

Audit

- Assist in the audit planning process and manage ICT and IG audit returns for the Trust.
- Ensure internal audits are undertaken to provide evidence to support the assertions of the Data Security and Protection Toolkit, such as Data Quality Completeness and Validity checks, Privacy by Design audits, efficacy and effectiveness of Access Controls.
- Ensure that there is effective external audit of the Trust's annual Data Security and Protection Toolkit evidence prior to submission to NHS Digital.
- Undertake audits as necessary to support the delivery of the Information Governance strategy, the Data Security and Protection Toolkit and Network and Information Security Regulation.

Annual Returns

- Ensure that all annual returns are meet the quality expectations of the Trust.

Key Result Areas
Information Governance

1. To design and specify associated standards for information governance arrangements and reporting of these activities, based on the Data Security and Protection Toolkit and Network and Information Systems Regulations requirements.

2. To maintain an up to date knowledge of Information Governance and related statutory changes and initiatives which affect the Trust and its clients

3. To provide Information Governance consultancy and advisory service to the Trust in a timely and auditable manner

4. To provide advice and assistance to Trust staff to comply with the Trust's Information Governance policies and procedures

5. To advise the Trust to implement and adhere to appropriate Information Governance and related policies adopting community wide standards as appropriate and in accordance with the IG Toolkit.

6. To work to establish effective IM&T disaster recovery and Business Continuity Plans and ensure such plans are reviewed and tested on a regular basis.

7. To deliver agreed arrangements for access and sharing protocols where clinical activities are delivered across the Kent and Medway Integrated Care System.

8. Plan and develop a strategy for the storage of sensitive personal information to include Health Records, X-Rays, Employee Records, Pay and Pension Records, and other records with due regard to the Data Protection Act and associated legislative requirements.

9. To work with the Head of Information to ensure a programme is in place to improve data quality standards in the Trust, and monitor and report progress to the relevant forum.

10. To manage Information Governance projects and programmes, and publish up to date Information Governance and Security related Trust policies which meet statutory requirements and NHS standards.

11. To work with Trust staff to ensure breaches in Information Governance including SIs are reported, investigated and resolved in a professional manner and those that require reporting to DH, ICO, and the CQC are done so in a timely manner

12. To work with other IG colleagues in other NHS Trusts and other external organisations to ensure a consistent approach to IG throughout the region

13. To develop and maintain IG Risk Register and ensure that all IG risks are alerted to the Trust Senior Information Risk Owner.

Information Governance Management

14. To monitor all Information Governance returns, including the Data Security and Protection Toolkit to the Department of Health, , and Secondary Uses Service for compliance with statutory requirements, ensuring they are submitted by the appropriate deadline.

15. To provide specialist advice and guidance on cross-organizational information security initiatives.

16. To provide specialist advice for assessing the adequacy and co-ordinating the implementation of specific controls for new systems, products or services;

17. To undertake or manage investigations and report on information security incidents to Trust senior staff, to involve Counter Fraud and other organisations as necessary.

Information Governance Training

18. To implement and maintain an Information Governance training framework for all staff that ensures all staff receive the relevant training according to the job role.
19. To monitor IG training received by all staff to ensure a programme of continuous improvement can be established and maintained.

Information Security

20. To provide a leadership role in developing the Trust's approach to Information security, both physical and cyber.

21. To coordinate specialist advice on information security from internal and external advisors and coordinate this throughout the organisation in accordance with ISO17799 controls.

22. To develop and maintain an Information Security Management System (ISMS) for the Trust.

23. To manage the creation and maintenance of an Information asset register as an integral part of the ISMS.

24. To work with the Head of IT to establish and maintain a Definitive Software Library (DSL) to track all software licensing for the Trust.

25. To manage the IG Risk Register, reporting to the

26. To support staff conducting IG aspects of internal and external audit programmes in respect of Information Governance activities.

27. To manage cyber security within the Trust to ensure that appropriate security measures (hardware and/or software) are contained within systems and networks for the prevention of unauthorised access from within the Trust and from external sources.

28. To report to the IG Committee on incidents, issues, security matters and current threats, vulnerabilities and steps taken to mitigate them.

Freedom of Information (FOI)

29. To manage FOI processes within the Trust to:
- ensure the Trust are aware of the latest FOI guidance

- ensure all Trust staff are aware of the FOI obligations

- facilitate a timely response to all FOI requests received.

Data Protection

30. To provide advice and guidance on all aspects of Data Protection to the Trust ensuring all staff are aware of their responsibilities.

31. To ensure all Trust systems and Information sources are registered with the Office of the Information Commissioner

32. Ensure the Trust has a robust framework of policies and procedures in place to ensure information is stored and shared according to Data Protection principles.

ICT Risk Management

33. Develop and implement the ICT Risk Management Strategy

34. Ensure that all ICT risks and incidents are managed and tracked to conclusion utilising the Datix Risk Management system.

35. Ensure all ICT staff are fully trained in Data Security and Protection policies and procedures.

36. Ensure all ICT Risk Management reporting requirements are achieved.

Accountability
Responsible for the strategic and operational management of Information Governance across the Trust, provide expert advice, develop and implement corporate policies and strategies following interpretation of national policies to ensure that the Trust meets its statutory and legislative obligations.

Communications and Relationships
The post holder will be required to deliver the Trust Information Governance strategy and work programme, communicating with both internal and external stakeholders, utilising negotiation, tact and diplomacy skills, often conveying highly complex, sensitive or contentious information to large groups or during one to one situations.

Planning and Organisational
The post holder will be expected to develop and implement an Information Governance strategy for the Trust with appropriate workstreams. Implementation of the strategy will require analysis of highly complex legislation, guidance and data and development of action plans and workstreams which may have unique characteristics to ensure that the Trust is able to meet targets and objectives.

Responsibility for Policy and Service Development
The post holder will lead the development of Information Governance related policies whose implementation will enable the Trust to meet its statutory and

regulatory/legislative obligations in relation to the integrity, availability and confidentiality of the data held.

Management Responsibility
The post holder will have direct line management responsibility for Cyber Security and Freedom of Information staff and will foster a culture of inclusion, positivity, trust and empowerment and will seek to encourage and develop staff to be the best that they can be.
The post holder will demonstrate the Trust vision and values in all they do and will exhibit a commitment to quality of care.
The post holder will promote learning and innovation, will demonstrate and encourage team working within MTW and across the wider Health economy and will strive to deliver an effective, high quality performance for the benefit of all patients and staff.

Physical Effort:
- A combination of sitting, standing and walking with little requirement for physical effort.

Mental and Emotional Effort:
- There is a frequent requirement for prolonged concentration where the work pattern is unpredictable with competing demands. The post holder will deals with staff performance and disciplinary matters and will provide advice in relation to Information Governance Serious Incidents and data breaches.
- The post holder will be party to very sensitive information and reports to regulatory organisations such as the Information Commissioner's Officer, Nursing and Midwifery Council and the General Medical Council.
  The role requires the regular involvement in the investigation of incidents providing expert advice to managers across the Trust and leading more complex investigations that may include criminal activities including the Computer Misuse Act.
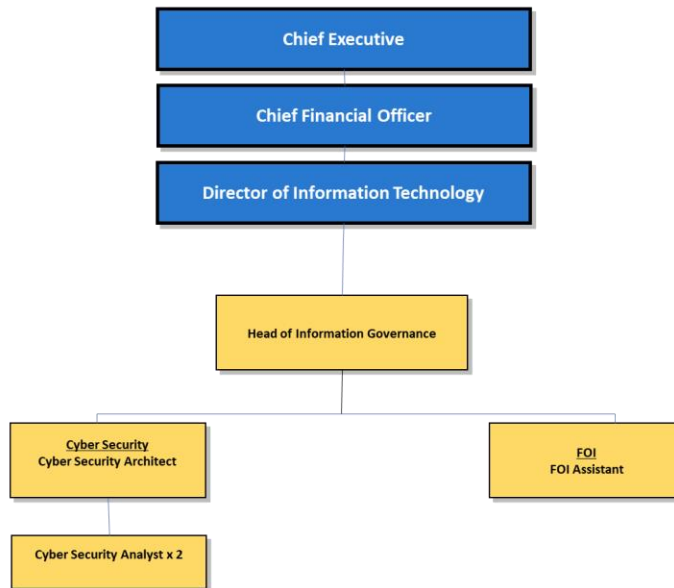
Research and Development
The post holder will undertake surveys and audits as necessary to support the delivery of the Information Governance strategy, the Data Security and Protection Toolkit and Network and Information Security Regulation. Such audits and research will be undertaken regularly, examples being research into new cyber threats and potential mitigations, audits of systems access (particularly in relation to allegations of breaches of privacy), IG awareness surveys.

Working Conditions
- Travel between Trust sites and across Kent and Medway and other areas in London and the South East Region to customer and contractor organisations.

Information Governance Team

```
┌─────────────────────────────────┐
│        Chief Executive          │
└─────────────────────────────────┘
                │
┌─────────────────────────────────┐
│     Chief Financial Officer     │
└─────────────────────────────────┘
                │
┌─────────────────────────────────┐
│ Director of Information Technology │
└─────────────────────────────────┘
                │
      ┌─────────────────────────┐
      │ Head of Information Governance │
      └─────────────────────────┘
        ┌───────────────┴───────────────┐
┌─────────────────────┐         ┌─────────────────────┐
│   Cyber Security    │         │        FOI          │
│ Cyber Security Architect │    │    FOI Assistant    │
└─────────────────────┘         └─────────────────────┘
          │
┌─────────────────────┐
│ Cyber Security Analyst x 2 │
└─────────────────────┘
```

Job Description Agreement:

Signature of post holder:_____
Date: _____

Name: _____

Signature of Manager: _____ Date: _____

Name: _____

Statement:

1. This job description is a broad reflection of the current duties. It is not necessarily exhaustive and changes will be made at the discretion of the manager in conjunction with the post holder.

2. Time scales for achievement and standards of performance relating to the duties and responsibilities identified in this job description will be agreed via the annual appraisal process with the post holder.

3. As an employee of Maidstone & Tunbridge Wells NHS Trust, the post holder will have access to confidential information. Under no circumstances should this be disclosed to an unauthorised person within or outside the Trust. The post holder must ensure compliance with the requirements of the Data Protection Act.

4. As an employee of the Trust, the post holder will be required to adhere to all Trust policies including Equal Opportunities where all employees are expected to accept individual responsibility for the practical implications of these policies.

5. The post holder is required to take reasonable care for the health and safety of themselves and others that may be affected by what they do while at work.

6. This post may require the post holder to travel across the Trust sites in the course of fulfilment of their duties.

7. The Maidstone & Tunbridge Wells NHS Trust has a no smoking policy.

8. Clinical Governance: You will be expected to take part in the processes for monitoring and improving the quality of care provided to patients. This includes risk management and clinical audit. If you engage in clinical research you must follow Trust protocols and ensure that the research has had ethical approval. You will be expected to ensure that patients receive the information they need and are treated with dignity and respect for their privacy.

9. All staff should be aware of their responsibilities and role in relation to the Trust's Major Incident Plan.

10. INFECTION CONTROL AND HAND HYGIENE - All Trust employees are required to be familiar with, and comply with, Trust policies for infection control and hand hygiene in order to reduce the spread of healthcare-associated infections. For clinical staff with direct patient contact, this will include compliance with Trust clinical procedures and protocols, including uniform and dress code, the use of personal protective equipment policy, safe procedures for using aseptic techniques, and safe disposal of sharps. All staff are required to attend mandatory training in Infection Control and be compliant with all measures known to be effective in reducing healthcare-associated infections.

11. All staff are required to fully participate in learning and development opportunities and ensure they remain compliant with statutory and mandatory training requirements throughout their employment with the Trust.

12. All staff are required to fully comply with the NHS Code of Conduct.

13. **SAFEGUARDING CHILDREN -** Everyone employed by the Trust regardless of the work they do has a statutory duty to safeguard and promote the welfare of children. When children and/or their carers use our services it is essential that all child protection concerns are both recognised and acted on appropriately. You have a responsibility to ensure you are familiar with and follow the child protection procedures and the Trust's supplementary child protection guidance which is accessed electronically on the Trust's Intranet site. You have a responsibility to support appropriate investigations either internally or externally. To ensure you are equipped to carry out your duties effectively, you must also attend child protection training and updates at the competency level appropriate to the work you do and in accordance with the Trust's child protection training guidance.

14. **SAFEGUARDING ADULTS -** Everyone employed by the Trust regardless of the work they do has a duty to safeguard and promote the welfare of vulnerable adults. When patients and/or their carers use our services it is essential that all protection concerns are both recognised and acted on appropriately. You have a responsibility to ensure you are familiar with and follow Trust policies in relation to safeguarding vulnerable adults. You have a responsibility to support appropriate investigations either internally or externally. To ensure you are equipped to carry out your duties effectively, you must also attend vulnerable adult protection training and updates at the competency level appropriate to the work you do and in accordance with the Trust's vulnerable adult protection training guidance.

15. All staff are required to provide the highest levels of service in their work and to adopt the highest standards of behaviour as stated and implied in the Trust Values of PRIDE.

Head of Information Governance
Maidstone and Tunbridge Wells NHS Trust
Person Specification

AREA	ESSENTIAL	DESIRABLE
Qualifications	Masters degree or equivalent knowledge gained through demonstrable experience of compliance to all relevant Information Governance standards including the Data Protection Act, ISO17799, Freedom of Information Act.	Masters degree in related specialist area. ISO 17799 accredited. Foundation Certificate in Service Management (ITIL Green Badge). PRINCE2 Foundation Certificate.
Experience	In depth and comprehensive knowledge and understanding of Information Governance issues in a large, complex and diverse operating environment. Strong organisational and change management experience. Knowledge and experience of leading the IG function across a large organisation such as a large Acute Hospitals Trust. Knowledge and experience of preparing Business cases and IG strategies for both medium and long term that support corporate objectives. Knowledge and experience of leading the ICT Risk Management function across a large organisation such as a large Acute Hospitals Trust Proven ability to work with and lead a team, demonstrating initiative, good	Experience of managing change in a fast moving environment. Experience of designing and implementing a fully documented Information Security Management System. Experience of working and engaging with clinical staff and other professional users.

	customer service skills and working to timescales with a flexible approach.	
	Managing client relationships at all levels.	
	Managing external relationships such as Social Services and Police.	
	Experience of large-scale procurements.	
	Management and control of budgets.	
	Demonstrable knowledge and experience of Business Continuity Planning and testing.	
	Extensive experience of writing policies and procedures.	
	Experience of Records Management systems.	
Knowledge	Detailed and extensive knowledge and understanding of all relevant IG related standards such as Data Protection Act, Freedom of Information Act, and ISO17799. Good understanding of the requirements for a comprehensive Information Management Security System. Good working knowledge of Business Continuity Planning and implementation processes and procedures. Good working knowledge of Microsoft Office products. Good working knowledge of Risk Management methodologies.	Detailed and extensive knowledge of the NHS IG Toolkit and Statement of Compliance. Knowledge of the Connecting for Health programme and its related IG issues. Knowledge of a Risk Management methodology such as CRAMM.

| Skills | Expert in Information Governance legislation and standards.

Proven ability to deliver pragmatic and effective solutions despite obstacles.

Flexible approach to problem solving.

Ability to manage Serious Untoward Incidents for the Trust and manage outcome.

Ability to communicate effectively in writing, face to face and over the telephone with a wide ranging audience including Board Directors, clinicians, technicians, managers and administrators

Ability to explain highly complex technical issues without using jargon.

Ability to plan, prioritise and delegate effectively.

Effective and confident public speaking and ability to prepare presentation material and deliver presentations.

Strategic thinker with the ability to translate strategy into operational systems.

Effective prioritisation skills including the ability to juggle multiple tasks and conflicting priorities and work under pressure to tight timescales.

Good negotiation and persuasion skills with particular ability to gain buy in from peers without direct authority.

An organised and methodical approach and attention to detail. | |

	Ability to deal with a full range of staff management activities including recruitment, training, mentoring, appraisals, conflict resolution, disciplinary proceedings etc	
Attributes	Customer oriented, confident, reliable, and approachable. A self motivated team player. Flexible and versatile with a pragmatic approach to finding solutions to a whole variety of problems. Patient and diplomatic. Ability to think widely and challenge existing or traditional ways of working. Enthusiastic, determined and energetic. Prepared to ask for and give help when needed. Willing and able to pass knowledge on and train other team members. A natural leader. Ability to remain calm under pressure. Willingness to take responsibility and do what is needed to get the job done. Completer/Finisher. A good listener with the ability to coach, coax, mentor and persuade all types of staff, colleagues and customer at all levels of seniority. Ability to lead serious security incident investigations	
Additional	Considerable travel across Kent and	

| requirements | Medway and other areas and the post holder must provide his or her own suitable transport, insured for business use

Flexibility in working hours/requirement to work additional hours from time to time | |

Date: June 2021