



THE NAIROBI HOSPITAL

Career Opportunity

The Nairobi Hospital, a leading health care institution in the region has an excellent career opportunity for an individual who possesses a passion for excellence, strong work ethic, results oriented and committed to continuous improvement. The successful candidate will be a team player, and well informed with the ability to effectively add value to enable good outcomes in line with our Strategic Plan (2019-2024).

DATA PROTECTION OFFICER

REF: TNH/HRD/DPO/11/2022

Reporting to the Head of Risk & Compliance, the successful candidate will be responsible for implementing and enforcing Hospital wide data protection compliance framework and systems to ensure the Hospital is compliant with the Data protection laws and regulations.

ROLES AND RESPONSIBILITIES

- Act as the primary point of contact within the Hospital for members of staff, regulators, and any relevant public bodies on issues related to data protection.
- Advise the Hospital and employees on data processing requirements provided under this Act or any other written laws.
- Establishing a Data Protection framework and implementation plan, amend existing internal data protection policies, guidelines, and procedures, in consultation with key stakeholders including developing templates for data collection and assisting with data mapping.
- Support the Hospital in preparation of privacy statements for each processing operation, and ensuring processes are put in place to ensure that the privacy statement is provided to data subjects on all Hospital forms and/or literature, websites and other communication or data collection mediums.
- Promote a culture of data protection compliance across all units of the Hospital.
- Collaborating with the Information Security function to maintain records of all data assets and exports and maintaining a data security incident management plan to ensure timely remediation of incidents including impact assessments, security breach response, complaints, claims or notifications and responding to subject access requests.

- Promptly informing the direct supervisor about possible threats and incidents impacting normal workflow and data processing.
- Hold trainings with staff members across different Hospital units who are involved in data handling or processing.
- Perform Data Protection Impact Assessments for projects and any new products and services where personal data will be processed.
- Proactively conduct audits to ensure compliance and address potential issues regarding data privacy.
- Maintain records of all data processing activities carried out by the Hospital.
- Serving as a point of contact between the Hospital and Regulatory Authorities and co-operating with them during inspections and co-operate with the data Commissioner and any other authority on matters relating to data protection.
- Interfacing with data controllers and data subjects to inform them about the use of their data, their data protection rights, obligations, responsibilities, the measures the Hospital has put in place to protect their personal information and to raise awareness on the above.
- Review vendor contracts to drive achievement of 100% inclusion of data protection clauses in partnership with Supply Chain, Information Security, and legal function.
- Ensure all queries from data subjects seeking to exercise their rights are responded to within required timeframes and required reports are timely filed with the regulator.
- Coordinate reporting of data breaches to data protection commissioner.
- Respond to all data protection queries on behalf of the Hospital
- Respond to any notice on data breach and make follow up for adequate reporting with lessons learnt for all identified data breaches.
- Work with management to prioritize business and information security needs.
- Identify and define new process improvement opportunities on data protection.
- Report on compliance gaps noted and ensure that the needed improvements are recommended.
- Work with legal team to ensure full compliance on all data protection laws.
- Providing quarterly status updates to senior and middle management and drawing immediate attention to any failure to comply with the applicable data protection rules.
- Any other responsibilities that may be assigned to the job holder by the supervisor from time to time.

EDUCATION AND EXPERIENCE

- Law degree from an accredited law school or Bachelor of Science in Computer Science or an equivalent of the two.
- Certified Information Systems Auditor (CISA) certification/ Certified Information Systems Security Professional (CISSP)/ Certified Information Security Manager (CISM) certification
- Have carried out at least one Data Protection Impact Assessment exercise

- Minimum of three years' experience working in a data protection compliance or a related field
- Strong project management skills
- Ability to work well under pressure and manage sensitive and confidential information
- Excellent verbal and written communication skills, with strong attention to detail
- Great interpersonal skills and ability to work well both independently and as part of a team

CORE COMPETENCIES

- Ability to provide legal advice and opinions
- Negotiation skills
- Drafting skills
- Communication skills
- Interpersonal skills
- Keen on learning new skills
- Team working skills
- Judgement and decision-making skills
- Planning and organising skills
- Integrity
- Confidentiality

If your background, experience and competence match the above specifications, please send us your application (cover letter & CV/Resume) quoting the job reference number, your current remuneration, testimonials and full contact details of 3 referees, to reach the undersigned not later than **15th December 2022**. Only shortlisted candidates will be contacted. We shall **ONLY** accept **ONLINE** applications and contact **SHORTLISTED** candidates.

The Nairobi Hospital does NOT charge recruitment fees.

Human Resources Manager
The Nairobi Hospital
P. O. Box 30026 – 00100
NAIROBI

Email: recruitment@nbihosp.org