COP403

GENERAL CONFIDENTIALITY POLICY AND PROCEDURE

Table of Contents

1. POLICY INTRODUCTION

National Ambulance (NA) places a high value on the responsibility to maintain confidentiality, both for the patients under their care and the business processes and financial dealings undertaken by all sectors of the organisation. It is, therefore, of prime importance that all NA employees and the organisation treat as confidential all information in relation to patients that is received by them and must not disclose or use that information other than for the purposes of the provision of healthcare services and treatment, except to the extent that it is permitted by other DoH regulations. This policy is related to the Management components, Leadership and Commitment, Risk Evaluation and Management and Continuous Improvement.

2. SCOPE

This policy applies to all National Ambulance employees and any contractors, consultants or others related to the organisation who have access to any confidential information. It applies to all information and systems detailed in the definitions below.

3. ROLES AND RESPONSIBILITIES

The Chief Executive Officer is responsible for oversight of management of information, for taking or delegating action to rectify any errors or omissions and to advise on any necessary revisions and improvements to ensure continual improvement.

All National Ambulance (NA) employees must be aware of the importance of confidentiality, how to protect it accordingly, and the types of information that are considered to be confidential.

All employees must sign, as part of their contract a Statement of confidentiality reading and understanding the definition above. Any NA employee who is proven to have breached this policy will be subject to disciplinary action as detailed in the Employee Contract, up to and including termination of employment.

All Executive members and managers mentioned below must carry out their roles for access and permissions to information in accordance with this policy and with reference to the table below.

Documentation	Responsibility
Accounting and Finance documents, whether stored in paper or electronic format	Chief Financial Officer
All other forms of information unrelated to Accounting and Finance	Chief Administrative Officer
All Clinical documentation	Medical Director
All Dispatch/Operations documentation	Chief Operations Officer

4. POLICY CONTENT

4.1. DEFINITIONS

Confidential Information includes: Patient related or Corporate related information, whether oral, electronic or written, of the Employer or its staff or business associates such as marketing practices, procedures and management policies, records, documents, accounts, plans, designs, specifications, software, correspondence, letters and papers of every description and electronically recorded data including, without limitation, any official information as prescribed by the Employer, and including all copies or extracts from any of the foregoing, within the Employee's possession or control relating to the affairs, transactions or business of the Employer or which may come into the Employee's possession in the course and by reason of Employment with the Employer, whether or not the same were originally supplied by the Employer.
Patient information : Any information pertaining to the patient including, written and electronic patient care records, specific reports, computer printouts, e.mail, databases, statistics, verbal communications such as patient handover and observations. Microfilm, X rays or scans, photographs, video, CD Rom or USB, log books, registers, faxes and e-mails.
Financial Information: Confidential financial information ('**Financial Information**') refers to all financial information created by, received by and / or submitted to the Finance Department of National Ambulance. Such Financial Information may include, but is not limited to, the Annual Financial Statements of the company, the monthly management reports prepared by the Chief Financial Officer, financial or other reports submitted to the Executive Management and / or the Board of Directors, financial or other reports submitted to the shareholders or regulators, budgets, forecasts, cash flow projections, all payroll-related information, revenues from clients (including the underlying contracts and other client specific information), payments to suppliers for goods and / or services received, tenders submitted to potential clients, and / or any other information that may under the circumstances reasonably be deemed to be of a confidential nature, the disclosure of which, either externally or internally, may cause harm, however defined, to the company.
Healthcare Information Systems A combination of vital and health statistical data from multiple sources such as patient care records, dispatch systems, metric data and audit, used to derive information about the health needs, health resources, use of health services, and outcomes of use by the people in a defined region or jurisdiction and derived from inputs using either written medium or electronic devices. The information systems contain features that hospitals need for daily business management such as patient tracking, billing, administrative programs and clinical features

4.2. PATIENT INFORMATION

It is the responsibility of all NA employees to protect the confidentiality of patient information regardless of the source of the information, including written and electronic patient care records, specific reports, computer printouts, e.mail, databases, statistics, verbal communications such as patient handover and observations.

Healthcare providers (facilities and professionals) must treat as confidential all information in relation to patients that is received by them and must not disclose or use that information other than for the purposes of the provisions of healthcare services and treatment. All confidential patient information, regardless of the medium it is stored on or the location it is stored at, is given the same level of protection, to include microfilm, X rays or scans, photographs, video, CD Rom or USB, log books, registers, faxes and e-mails.

The patient care record is a confidential document that details personal medical information for the patient. Due to the sensitive nature of the information being recorded access to the records must be limited to those who have a patient care role. The only exception to this is where records are being used for audit purposes; every effort should be made to anonymise any audit detail as well as to protect the patient details from staff that do not have a role in patient care or audit.

NA employees including healthcare professionals and other involved personnel need access to patient records to carry out their duties; this access must be appropriate to the scope of each employee's job duties. Duties must be included in the position description and must be emphasised at induction and training sessions and throughout their time in employment.

Staff members who have access to patient information must not share this information with others who are not involved in the care or treatment of patients or in evaluation of the care and treatment given.

Specific release of patient information must be followed including compliance with DoH regulatory Requirements relating to the-

- Right of a patient to access, by obtaining a copy of that data,
- Right of a patient to require that data to another healthcare facility or professional,
- Restrictions on the collection use retention, storage and destruction of data relating to healthcare in Abu Dhabi;

All National Ambulance Policies and Procedures including but not limited to CGP103 Patients' Rights and Responsibilities Policy and Charter, CGP105 Consent Policy and any applicable Laws and Regulations must also be taken into account.

Any information released to a third party in accordance with the above requirements will be subject to anonymising and redacting to protect patient confidentiality by the Medical Director

Access to patient records for research purposes, audit or statistics will be controlled by the Medical Director. The NA audit activities must follow the QHP202 Audit, Inspection and Non-conformance Policy and Procedure and CGP148 Clinical Audit Policy and Procedure.

4.3. HUMAN RESOURCES/ ADMINISTRATIVE INFORMATION:

All personal information about a National Ambulance employee is considered confidential and should not be discussed or communicated to anyone outside of the Human Resources/Administrative Department unless required in the course of the Company's business process.

Confidential information in the Human Resources Department includes employee information including but not limited to the following: Birth date, marital status, spouse name, children's names and ages, telephone numbers, contract details, salaries and benefits, CVs, performance reviews, performance action plans, disciplinary issues/action taken, terminations and all other sensitive information about an employee.
Human Resources employee files must be maintained in a secure area with access limited to authorized employees only.

4.4. FINANCIAL INFORMATION

All Financial Information about National Ambulance is to be considered confidential and should not be discussed or communicated to anyone outside of the Finance Department, unless the sharing of such information is required during the

course of official business. For any questions as to what may reasonably be considered Confidential Financial Information the reader is requested to seek the advice of the Chief Financial Officer and / or the Chief Executive Officer before making use of the information that may have been obtained, no matter the source of such information.

4.5. HEALTHCARE INFORMATION SYSTEMS

All patient information is confidential. Executive members and managers or their official delegates shall be responsible for determining and assigning appropriate employee access to health information system modules including the electronic patient record, and dispatch systems that contain patient details as relevant to their specific job functions within the organisation.

Orientation regarding systems access shall be provided to Executive members and managers or their official delegates, prior to the assignment of authorization privileges.

Computer user ID, passwords or other types of system access authorizations are assigned on an individual basis and must not be shared with anyone. Users must take all reasonable precautions to protect the privileges assigned to them.

Each user is responsible to ensure that their workstation or device is safeguarded and protected from unauthorized access and viewing and ensure that they fully log off from the workstation or device when their transactions are completed or when leaving the work station or device for a period of time in line with ITP121 Clear Desk Clear Screen Policy.

Users must be aware that there is no guarantee of complete privacy or security when using electronic communications therefore the utmost vigilance is required to avoid the circulation of patient specific information by email or other electronic communications.

All National Ambulance staff, contractors, consultants or others related to the organization must report to the Knowledge management personnel or to the IT Manager any instance of improper or potentially illegal use of the electronic information system.

Database users or coordinators are responsible for preparing a user password confidentiality system to be communicated and agreed to by each user prior to being given access to the specific database.

Upon termination of any National Ambulance employee, the direct line manager or their official delegate is responsible for deleting access to all applications and access to all devices and organisation information for that employee effective, at the latest on the last working day for the employee in line with ITP125 IT Operations Policy and HRP104 Leaving Employment Policy and Procedure.

4.6. 998 CALL RECORDINGS, CCTV RECORDINGS, BIOMETRIC ACCESS DATA

All 998 Call recording and CCTV recordings should be treated as confidential. Executive members and managers or their official delegates shall be responsible for determining and assigning appropriate employee access to 998 Call and CCTV information including the audio record, video content as relevant to their specific job functions within the organization.

Access to Biometric access data shall be via the relevant management applications by managers for their relevant teams.

Internal Access to 998 Call and CCTV recorded information will be provided by authorization from the Chief Administration officer.

External access to 998 Call, CCTV recording and Biometric Data will be provided in compliance with UAE Law and will be facilitated following a written request from CID and approval from the Chief Administration officer.

All National Ambulance staff, contractors, consultants or others related to the organisation must report to the Knowledge management personnel or to the QHSE manager any instance of improper or potentially illegal use of the electronic information 998 Call and CCTV recordings.

5. RELATED POLICIES AND FORMS

List related policies and procedures to the created/updated policy.

Policy & Procedure /Form
COF311 Educator Acknowledgment and Non Disclosure
CGF180 Patient Care Record Folder Confidentiality Agreement
ITP121 Clear Desk Clear Screen Policy
CGP148 Clinical Audit Policy and Procedure
ITP125 IT Operations Policy
ITP121 Clear Desk Clear Screen Policy
HRP 104 Leaving Employment Policy and Procedure

6. FEEDBACK

Any feedback or suggestions for improvement to this Policy, Processes or Procedures can be submitted to qhse@nationalambulance.ae

7. DOCUMENT CONTROL AND OWNERSHIP

A review and update of this document will take place as necessary, when changes occur that identify the need to revise this Policy such as changes in roles and responsibilities, release of new legislative or technical guidance, or identification of a new policy area.

This document ownership for editing is identified as:

- Chief Executive Officer

Change Brief

Version No.	Date	Changes
1	14-January-14	First Version
2	29-May-14	Migrated to Corporate Services
3	February 2017	Review against updated legal register, no changes required
4	April 2017	Updated to include 998 Call, CCTV and Biometric data access
5	February 2020	Due to review, removed Chief Medical Director, added Medical Director. Education Department Statement of Confidentiality & Non-Disclosure
6	September 2020	Removed the Education Department Statement Added COF311 Educator Acknowledgment and Non Disclosure & CGf180 Patient Care Record Folder Confidentiality Agreement under related policy section. *Change the format to match the Policy and Procedure Template* *Change subcontractors to contractors* *Add reference to ITP121 Clear Desk Clear Screen Policy* *Add reference to Clinical Audit Policy and Procedure CGP148*

		Add reference to ITP125 IT Operations Policy and HRP104 Leaving Employment Policy and Procedure. *Add clause numbers to the sub sections* *Change HAAD to DoH*

CEO Approval

Board Member Verification