COP 420

ELECTRONIC CORPORATE COMMUNICATION POLICY AND PROCEDURES

Table of Contents

1. POLICY INTRODUCTION

This Policy aims to ensure the security of the information exchange at National Ambulance internally and externally.

2. SCOPE

This policy applies to all National Ambulance employees.

3. ROLES AND RESPONSIBILITIES

1. **Chief Executive Officer or his delegate:** responsible to approve non-medical information shared with external stakeholders.

2. **Medical Director:** responsible to approve medical information shared with external stakeholders. When authorized by the health sector regulator of Abu Dhabi

3. **Human Resources and Corporate Services Manager:** is responsible to support the IT Department in defining the controls and ensuring the employees adherence to the policy and the relevant disciplinary action in case of the breach of the policy.

4. **HR Department:** is responsible to conduct awareness about the policy to all users during on boarding process and responsible to communicate the need for activation and deactivation accounts.

5. **IT Department:** is responsible to ensure the protection of communication infrastructure, and establish integration methods, maintain the security level of the electronic or online transactions and business information systems, identify and implement security requirements for exchanging information and software internally/externally**.**

6. **All National Ambulance Employees:** are responsible to read, understand, and adhere to this policy in their day to day activities.

4. ELECTRONIC CORPORATE COMMUNICATION POLICY

4.1. ACCOUNT ACTIVATION AND DEACTIVATION:

4.1.1. ACCOUNT ACTIVATION:

- All staff User accounts to be created based on the request of HR or relevant department heads approval.
- Third Party accounts to be created on the approval of the Chief Executive Officer or Delegated authority
- Service accounts will be managed and maintained by IT to the required level to maintain service availability and security.
- Generic or group emails account should have an owner to ensure the accountability of the information exchanged internally or externally.

4.1.2. ACCOUNT DEACTIVATION:

- Deactivation of user accounts should be raised by HR or relevant department heads
- Deactivation of service accounts will occur once the service maintained by these accounts is no longer required.
- The account deactivation communication to be initiated by HR department during the following circumstances:

- Employee Resignation or End of Contract.
- Transfer, if needed to be removed from group emails account.
- If requested by the relevant department heads or executives.
- In case the user breached or misused the provided access in any mean
- In order to prevent data loss or dissemination of protected information

4.2. Information Exchange Agreement

National Ambulance can only participate in a clinical Information Exchange Platform if authorized to by the Chief Executive Officer, Medical Director, and the Clinical Ethics Working Group with prior approval from DoH/MoH.

The content of the information exchange agreement is specified in COP424 Third Party Policy. Access to the approved Information Exchange Platform should be authorized and provided based on need to know basis. Access should be periodically validated and access requirements verified. Information Exchange Platform usage should be periodically audited and any misuse or incidents should be reported to Health Information Infrastructure Protection Working Group, health information exchange operator, and DoH/MoH.

4.3. General usage:

- All accounts, emails addresses, or any tool of communication resources provided by National Ambulance should be used for official purpose only.
- NA staff should avoid using the provided communication tools for personal communications/correspondences.
- All Users shall be held responsible for any misuse of electronic communication correspondences from their accounts, if proven to be as an intentional act from the User.
- Users shall refrain from initiating or participating in any electronic communication or newsletters not related to the job duties, such as forwarding chain emails whether commercial or with personal amusement and entertainment content
- Users shall refrain from sending information, software, files or attachments that are illegal or unauthorized, or include any defamatory, offensive, racist or obscene remarks.
- Users shall refrain from accessing or using any electronic communication account of other Users, unless it is authorized/delegated by the account owner with proper business justification and this shall be requested from and processed formally by the relevant department executive responsible and without sharing the password of the account.
- User shall refrain from publishing clinical data unless it's approved by the Clinical Ethics Working Group in accordance with CGP207 Clinical Ethics Internal Working Group and CGP109 Policy and Procedure on Clinical Ethics
- Users shall refrain from using personal emails for official communications/correspondences.
- Staff will use the National Ambulance provided email address when communicating to third parties regarding National Ambulance business or activities.

4.4. Disclosure of Confidential Information

National Ambulance is committed to providing timely, accurate, and complete disclosure of its necessary company information properly. All department heads should ensure the protection of protected information for each department and monitor the access to such information.

Disclosing confidential information externally is strictly prohibited unless authorized to by the Chief

Executive Officer or Delegated authority, as detailed in the COP403 General Confidentiality Policy, COP401 Information Management Policy, and COF130 Non-Disclosure Agreement, which should be signed by all staff members upon the assumption of duty in accordance with HRP104 On- Boarding and Induction Policy and Procedure.

Removable media used to store confidential information, whether for internal or external purposes, shall be encrypted in accordance with ITP102 Acceptable Use of Assets Policy. If transported to a third party then the media should be placed in an envelope marked restricted access. The individuals transporting the removable media should either be a staff from National Ambulance or a reputable courier that offers secure transport and allows tracking of the media in transit.

Confidential information should not be transmitted or shared through the internet, whether internally or externally, unless encrypted.

Confidential healthcare information is not to be transmitted outside the UAE

The encryption/decryption key, token, or password to access the encrypted data should be shared with the targeted person/s using a different communication channel than the channel to access the information.

Any violation or abuse of the communication guideline set out at National Ambulance may result in disciplinary actions.

5. RELEVANT LEGISLATION

International, federal, or local legislation and circulars relevant to this Policy. Full detail on this legislation can be found in QHP109 Legal Register.

Code, Name of Legislation	Jurisdiction
ADHICS	Abu Dhabi
DoH standard on Patient Healthcare Data Privacy	Abu Dhabi

6. RELATED POLICIES AND FORMS

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

Policy & Procedure /Form
COP403 General Confidentiality Agreement
COF310 Non-Disclosure Agreement
COP401 Information Management Policy
CGP207 Clinical Ethics Internal Working Group
CGP109 Policy and Procedure on Clinical Ethics
COP424 Third Party Policy

7. FEEDBACK

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

8. 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:

- HR & Corporate Service Manager

This controlled document is managed / overseen by [Procurement and Tendering Committee and/or Audit and Risk Management Committee and/or HR and Compensation Committee].
P

Change Brief

Version No.	Date	Change
1	April 2021	*New Policy*

CEO Approval

Board Member Verification