COP401

INFORMATION MANAGEMENT POLICY

Table of Contents

1. POLICY INTRODUCTION

The purpose of the Information Management Policy is to detail the current information environment at National Ambulance (NA) and to highlight future projects as well as describe staffing supporting information management.

The policy's aim is to provide information to meet the needs of all National Ambulance staff including those who provide clinical services, those who manage the Corporate Affairs, Clinical Governance and Operations, and those outside National Ambulance who aim at enhancing services and care provided by the organization to our patients.

By providing accurate, meaningful, comprehensive and timely information, it will assist decision makers in transforming information into knowledge, decisions, thus facilitate making the right actions at the right time.

The overall aim of the Policy is to enable National Ambulance to achieve continuous improvement in

- Identifying the organization's information needs
- Defining and capturing data and information
- Analyzing data and transforming it into information
- Maintaining the confidentiality of information
- Transmitting and reposting data and information
- Integrating and using information
- Validating data

National Ambulance will respond to any direction form UAE Governmental bodies with regard to appropriate control processes and procedures to ensure confidentiality, integrity, availability and retention of electronic records, payments and fees in accordance with Federal Law No. (1) Of 2006.

This policy is relevant to the Leadership and Commitment, Organizational Roles and Responsibilities, Risk Evaluation and Management, Implementation Monitoring and Reporting, Managing of Non conformances and Action Items, Auditing and Inspections, and Continuous Improvement Management System Components.

2. SCOPE

The Information Management Plan addresses all information assets including clinical, operational, administrative and financial data resources,. There are many mediums for data within National Ambulance, and many of these resources are controlled by the two main information repositories (IT department & Operations).

Information is generated and used during National Ambulance's operations, including patient care and for managing a safe and effective organization. The information management plan incorporates data and input from a variety of sources including;

- Clinical Service Delivery staff i.e. EMT-B, EMT-I, EMT-P
- Dispatchers
- Support departments
- Senior Leadership and Management
- External Organizations or external individuals

Clinical information/documents are included in a patient-specific clinical record both in paper and electronic format which integrates data from clinical processes, ancillary services, and clinical guidelines or evidence based practices.

3. ROLES AND RESPONSIBILITIES

The policy will be implemented and administered as follows:

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

1. CHIEF EXECUTIVE OFFICER

Is accountable for oversight of management of information and is responsible for taking or delegating action to rectify any errors or omissions and to advise on any necessary revisions and improvements to ensure continual improvement.

2. MEDICAL DIRECTOR

Is responsible for any related Clinical Policies, Procedures and Guidelines and any Clinical Performance Indicators. In addition, the Medical Director is accountable for the validity of clinical information and data released to public and is responsible for the oversight and monitoring of clinical data confidentiality and privacy

3. CHIEF OPERATIONS OFFICER

Is responsible for the implementation and monitoring of this Policy and Clinical Guidelines. In addition, the Chief Operations Officer is accountable for the validity of operational information and data released to public.

4. CHIEF ADMINISTRATION OFFICER

Is accountable for the validity of admin information and data released to the public. In addition, the CAO is responsible for ensuring the data audit process is followed by all staff.

5. CHIEF FINANCIAL OFFICER

Is responsible as Chief Information Security Officer (CISO) for ensuring National Ambulance compliance with the relevant legal requirements for data confidentiality and security and reporting noncompliance findings of audits and regulations.

6. ALL MANAGERS

Are responsible for ensuring that staff have induction in alignment with this Policy and Procedures, for monitoring the applicability and ongoing implementation and ensuring that all data related processes and policies are followed.

7. ALL STAFF THAT PROVIDE CARE FOR PATIENTS

Are responsible for acting according to this policy and procedures. They are also responsible for ensuring that they attend or pursue any relevant training recommended by their Managers. (I.e. face to face or online training). This includes staff supporting operations functions i.e. dispatchers.

4. POLICY STATEMENT

4.1. Goals and Objectives

Goal One – Support Patient Care
To support decision making in improving patient outcomes, improving health care documentation, assuring patient safety, and improving performance in patient care, treatment, and services

Objectives:

- Address the main clinical documentation requirements.
- Enhance prompt and rapid access to clinical information by the clinical staff through providing Information accurately, with acceptable turnaround time to facilitate healthcare process.
- Ensure that physicians and the clinical staff have appropriate skills, knowledge, and educational opportunities to effectively utilize information resources, such as internet access, appropriate clinical journals, and exposure to the latest evidence-based new practices.
- Protect the confidentiality and privacy of patient information, and ensure the availability, integrity, accuracy, and security of Clinical Information.

Goal Two - Support Administrative Decision Making
To provide timely and reliable information to decision makers, including statistics, and trends.

Objectives:

- Develop a computer based statistical module to support administrative staff in decision making.
- Provide office automation tools (including but not limited to electronic mail) to streamline processes.
- Promote the use of electronic resources for analysis, capturing storing and analyzing data.
- Provide decision makers and staff within National Ambulance proper training on information management prospective
- Recommend and support disease coding strategies to assist with data extraction and interpretation.

4.2. Planning

Main User Groups
For the purposes of defining key user groups the following have been identified within National Ambulance as the key users of the Information Management Policy. Other groups can be added to this at a later stage should the need arise.

- Clinical Service Delivery staff i.e. EMT-B, EMT-I, EMT-P
- Dispatchers
- Senior Leadership and Management
- External Organizations or external individuals

4.3. Confidentiality, Security and Integrity of Data

Information and data will be accessed on a need to know basis. All staff and patients have the right to privacy in accordance with the National Ambulance Policy COP403 General Confidentiality Policy; the policy clearly sets out the obligations for the confidentiality, security and integrity of patient data. Non – Disclosure Agreement describes the importance of confidentially and the breach of NDA agreements.

Owners of data that is regulated by an authority, e.g. ADHICS, will be handled as required by those laws including informing the authority of any issues, outages, and breaches as required by the authority. Any deviation from these laws and regulations should be approved by the respective authorities, including reporting any deviation from the data privacy standard to DOH. Breach of any of these legal and regulatory requirements may lead to regulatory action and sanctions from the respective authorities.

4.3.1. Information Classification Criteria

In compliance with ADHICs requirements, information assets will be classified based on the following classification factors and coloring themes:

Asset Classification	Classification Factor and Criteria
Public C100 M0 Y100 K0 R0 G150 B64 # 009640 GREEN	Information destined to be used in public domain or public use, and has no legal, regulatory, or organizational restrictions for its access and/or usage. Intended purpose from the creation, access and use of the information is the general advancement of society, promotion of the interest of the organization and of the country, providing essential information equipping citizens, patients and other stakeholders understand better the country's / governmental / organizational vision and values. E.g. Information posted on website and social media, Information used in seminars and conferences, research publications, anything sent externally that isn't covered by an Non-Disclosure Agreement
Restricted C100 M0 Y0 K0 R0 G158 B227 # 009EE3 BLUE	Information that must be afforded limited confidentiality protection due to its use in the day-to-day operations. Disclosure of such information could have limited adverse impact on the functioning or reputation of the entity or the government/health sector. Information that relates to the internal functioning of the entity and will not have general relevance and applicability to a wider audience. Although individual items of information are not sensitive, taken in aggregate they may reveal more information than is necessary if they were to be revealed. E.g. Policies and controlled documents, dispatch records, summary reports (clinical audit analysis), financial records
Confidential C0 M80 Y95 K0 R232 G78 B27 # E84E1B ORANGE	Information that requires robust protection due to its critical support to decision-making within the entity, and across health sector and government. Information that could disclose designs, configurations, or vulnerabilities exploitable by those with malicious intent. Information that the entity, or through government or regulatory mandates, has a duty of care to others to hold in safe custody e.g. critical personal information, health/healthcare information, government information, financial information etc.
Secret C0 M100 Y100 K0 R227 G5 B19 # E30513 RED	Information that requires substantial and multilevel protection due to its highly sensitive nature. Disclosure of such information could have a serious and sustained impact upon the government, national security, social cohesion, economic viability and health of the country. Information disclosure could potentially threaten life or seriously prejudice public order.

Table source DOH/SD/ADHICS/0.9

4.3.2. Protectively marking and identification of information assets

Information assets created and managed by National Ambulance will be identified according to 4.3.1 information classification criteria. Data owners must ensure that the information they manage and falls under their department is marked according to the criteria noted above.

National Ambulance Infrastructure is not equipped or approved for the creation, receipt, storage or transmission of secret information resulting in no secret information being used/managed in National Ambulance. National Ambulance doesn't label public information assets. Empty/clear forms, templates, and checklists that are labelled as confidential are to be treated as restricted information assets until they are filled.

4.3.3. Access Controls

Information access controls will be maintained to ensure that only authorized users have access to information assets as required to complete their normal working tasks by group and rights assignments.

Employees whose roles change or are terminated, will have access permissions removed or changed according to their new assignments in accordance with ITP125 IT Operations Policy.

Physical Access Controls will be installed to prevent the unauthorized access to physical information and data stores as defined in policy QHP213 QHSE Work Location Management Policy.

Device Access Controls, marking and banners will be placed on all assets that create, manage store or access information assets to ensure only authorized use of the asset occurs including:-
Protective Marking
Information Banners requiring acceptance of security terms of asset use
Screen Savers / Lock screens

In accordance with policy ITP119 IT Access Control Policy

Assets which are used in the emergency response or treatment of patients are exempt from any controls which may endanger patient safety by the possible delay or interruption of care needed to unlock or reactivate systems. Including but not restricted to:-

- AEDs / Defibrillators
- Radios and Mobile communications devices
- Mobile Data Terminals (MDTs) / Ambulance data terminals
- 998 Response communication, call logging and dispatch equipment

User Access Controls will be followed to prevent unauthorized access to information including:-

- Named user access with unique passwords
- No group / shared accounts
- Session Time out
- Screen Savers / lock screens
- Password Expiration

4.4. Confidential Information Assets

The following outlines the controls in place governing the main confidential information assets held by National Ambulance. In all cases access to these records must be given to individuals who are:-

- Current Staff who are authorized to access the records with a current signed NDA agreement
- Approved external Organizations or individuals with an approved current NDA agreement
- Individuals in possession of a court order or other valid legal document validating their request for access of the records.

- Other individual with a right by UAL law to access their own or family members information.

4.4.1. Patient Care Records

The Patient Care Record (PCR) is a legal document and is also part of the patient's health care record. Therefore, it is important that all patient care documentation produced by NA is clear and concise. The PCR must be completed after any call out, regardless of whether there has been patient contact or not; this includes standbys. Irrespective of how transient the patient intervention a full record must be completed.

The CGP119 Patient Care Documentation and Patient Care Record Policy and Procedure details:

- Who is authorized to make entries in the PCR
- Who can revise the content and form
- Who can review and Audit the Patient Care Documentation and PCR
- How Patient Care Documentation and PCRs are to be completed including identification of the author, date and time that the record was created.

4.4.2. Dispatch Records

Dispatch records provide an important reference for actions undertaken by dispatchers in support of NA Clinical Operations. Therefore, it is important that all dispatch documentation produced by NA is clear and concise. Dispatch records must be completed for all interactions between field staff and the Ambulance Communications Centre.

Ambulance Communication Center Procedure OPP113 details:

- Who is authorized to make entries in Dispatch Log
- Who can amend the Dispatch Log content and form
- How the Dispatch Log is to be completed including identification of the author, date and time that the record was created.

4.4.3. Vehicle Records

Vehicle maintenance records, both preventative or as a results of faults, are provided to National Ambulance as hard copies. Once received, these documents are scanned and inserted on OPIQ as attachment. Hard copies are filed into the respective ambulance file in the National Ambulance warehouse.

Other vehicle records uploaded in OPIQ and saved in their respective hard copy files include:

- Annual DoH certificates
- ADNOC technical test
- Annual registration
- Job cards
- Corporate vehicles and leased vehicles log

4.4.4. Video Surveillance Systems

Video storage will follow as a minimum the Abu Dhabi Monitoring and Control Centre Guidelines of 30 days history. Technical specifications and quality of capture will also be determined by the standard.

The IT Help Desk is responsible for maintaining the system and will rectify problems within one working day or report the failure to the Monitoring and Control Centre.

Access to view the systems must be approved by the CAO, or CEO in writing or by email.

Changes to the CCTV systems must by managed by IT through the COP414 Change Management Policy.

4.5. Documentation Retention Of Records, Data, And Information

The Document Retention Policy and Procedure COP402 in accordance with DoH Standard On Patient Healthcare Data Privacy includes all records and documents, regardless of physical form. It contains schedules for how long certain documents should be retained and how records should be destroyed. The policy is designed to ensure compliance with the regulations of the United Arab Emirates, to eliminate accidental destruction of records and to facilitate the organization’s operations by promoting efficiency and freeing up storage space.

It is the policy of National Ambulance:

- To comply with applicable legal and regulatory duties to retain documents
- To maintain the highest standards of data security, storage, and integrity
- To possess all documents required for normal business purposes, including administration of ongoing business relationships

National Ambulance directs and expects all officers, directors, employees, contractors and / or volunteers to follow the rules and procedures set forth in this document. ‘Documents’ include not only documents in paper form, but e-mail messages and all other forms of electronically stored information.

No officer, manager, employee, contractor and / or volunteer of National Ambulance shall knowingly destroy a document with the intent to obstruct or influence the investigation or proper administration of any matter within the jurisdiction of any Interest Person, as defined earlier in this document. This policy covers all records and documents of National Ambulance.

National Ambulance reserves the right to amend, alter and / or terminate this policy at any time.

4.6. Reporting And Use Of Data Within National Ambulance

Information is shared within the Executive Group through the weekly management team meetings and quarterly through Board Reports. Operations Staff provide weekly updates to the Chief Operations Officer across a number of performance indicators; these can vary between contracts and are subject to change with approval from the relevant stakeholder.

Other information such as Staff Satisfaction Surveys and Financial and Administrative reports are produced in accordance with the business need of the organization by the Chief Administrative Officer and Chief Financial Officer.

As part of the continual improvement process opportunities to refine and improve data presentation are available. It should be noted that appropriate change management controls will be in place to ensure the ability to examine data on a historical basis.

During the establishment of any project and as part of the ongoing commitment to continuous improvement both clinical and managerial information is integrated to support National Ambulance’s leadership and corporate governance. The main venue for this collaboration is through the weekly executive meeting and quarterly board meetings.

4.7. Selection Of Information Technology Resources

Before the acquisition of new technology platforms is commenced proposals must be tabled at the weekly executive meetings. The proposal should indicate the following.

- Why the platform is required.
- Benefits to the organization
- Patient Impact Assessment
- Type of platform required including overview of competitor.

- Estimated Costs
- Warranties and Support

Before a final decision is to be made support for the platform must be given by the

Medical Director	(Clinical Acceptance)
Chief Operations Officer	(Operations Acceptance)
Chief Financial Officer	(Budget Acceptance)
Chief Administration Officer	(System Acceptance)

4.8. Information systems governance and service ownership

All services and information systems must be identified in National Ambulance Business Service Catalogue with the following identifications: -

- **Data Classification Level** - Highest level of data classification allowed
- **Type of Service** – Business service, Technical Service, Application, ect
- **Business Owner** - Ultimately accountable for defining the required service value. Approves changes which impact service value and business risks.
- **Service Manager** - Responsible for assuring / maintaining the service value. Approves minor / medium changes so long as there is no change to the service value or impact to the business, responsible for ensuring the licenses are provided and the service is managed to the required levels and compliances
- **Service Provider** – Responsible for providing and maintaining the service. Manages and implements approved changes, provides value reports as to the service performance ensures the service is licensed and the current supported versions etc.
- **Service Administrator / Support** – supporting the service with issue / incident / problem management and training solutions.
- **Content Owner** – Oversees the creating and maintaining of content, usually approves access to that content
- **Content Approver** – Usually one of the above, approving content published to internal / external audiences.
- **Super User** – User with additional privileges and responsibilities in a system usually regarding content or user configuration
- **User** – Person or groups who consumes or uses the service provided with privileges consistent with their BAU needs.

4.9. Access to Information

Staff may only access information they are entitled to access in accordance with the COP403 General Confidentiality Policy.

Staff should sign the non-disclosure agreement yearly, and ensure they are conversant with their responsibilities and user obligations.

The IT department conducts periodic information security awareness sessions to ensure the compliance of all NA staff in liaison with clinical services.

4.9.1. Who can access, document and use the Patient Care Records:

- **Clinical Staff with DOH or MOH license under NA** are authorized to make entries in the PCR and other patient related documentation in accordance with their scope of practice and agreed competencies.
- **Clinical Administrative Assistant** does timely scanning, renaming, filing and archiving of the PCRs (paper PCRs, missing PDFs of ePCR, CAOS and ECG papers or other documents wherever applicable). Collecting PCRs and ePCRs of MVA's for insurance claims
- **Clinical Auditors** are authorized to review the patient care report for the clinical audit purposes.

- **Clinical Governance & Audit Officer** is authorized to review the patient care report for the clinical audit purposes & other related concerns /feedback.
- **Insurance & External Communication Manager** is authorized to access patient care report for the insurance claim purposes.
- **Insurance Claim Officer** is authorized to access patient care report for the insurance claim purposes.
- **Insurance Claim Assistant** is authorized to access patient care report for the insurance claim purposes.
- **IT Staff** in relation to development, maintenance and support and report generation purposes.

4.9.2. PROCESS IN CASE OF PATIENT/GUARDIAN OR AN AUTHORIZED ORGANIZATION REQUEST PATIENT CARE RECORD (PCR)

- Any patient/Guardian requesting any patient related documentation should be managed in accordance with NA information management policies and using "CGF137 – Patient Care Records Request Form"
- Patient's/ Guardian Passport or Emirates ID should be attached with the request.
- Signature of the requesting personnel should match in both Passport/Emirates ID and on the request form and this should be checked by the QHSE Assistant and then double checked by the Clinical Governance & Audit Officer
- The patient related documentation sent to the requested personnel as an encrypted document (with password) after Medical Director approval.

4.9.3. PROCESS IN CASE OF AN AUTHORIZED ORGANIZATION REQUEST PATIENT CARE RECORD (PCR)

- An Authorized Organization (e.g. police, Court) should send an official email to request any patient related documentation or report.
- The patient related documentation sent to an authorized organization (e.g. police, Court) as an encrypted document (with password) after Medical Director approval.

4.9.4. PROCESS FOR INSURANCE CLAIM

- Patients General Information: EID, Insurance card details and DOH license of EMT.
- Whole or part of the ePCR with appropriate police report if required.
- Diagnosis/Symptoms of the Patient: In ICD 10 code format.
- Activity Management part of ePCR in CPT and HCPCS code format.
- Medical Claims, files are submitted to DOH through the appropriate claims portal.

4.9.5. ACCESS CONTROLS

Data asset managers and owners, along with service owners will identify the level of access and access control for staff required to prevent unauthorized access to information based on the following (not limited to).

- Business requirement
- user roles and responsibilities
- Application and operating systems usage and access.

4.9.6. TERMINATION OF ACCESS

Termination of access to National Ambulance data assets will coincide with any of the following conditions are in place: -

- Employees end of employment,
- expiration of company NDA
- Request by an Executive

- In the case of an investigation, HR / Contract dispute, or other legal reason.

Reinstatement of access may be granted when the above conditions no longer apply.

4.10. PROTECTION OF RECORDS

Employee records – and other administrative information is kept within the Corporate Services area in secured cabinets. The HR & Corporate Services Manager is responsible for ensuring these files are secured on a daily basis. Electronic records are maintained on the N: Drive, access to the Corporate Services Section of the N drive is only granted by the Chief Administrative Officer. Records maybe signed out by staff on an as needed basis, final approval is with the HR & Corporate Services Manager for any access.

Financial records – and other finance information is kept within the Finance area in secured cabinets. The Chief Financial Officer is responsible for ensuring these files are secured on a daily basis. Electronic records are maintained on the N: Drive, access to the Finance Section of the N drive is only granted by the Chief Financial Officer. Records maybe signed out by staff on an as needed basis, final approval is with the Chief Financial Officer for any access.

Clinical records – Clinical records are defined as having a direct impact on patient care. Electronic records are maintained on the N: Drive, access to the Clinical Section of the N drive is only granted by the Medical Director. Records maybe signed out by staff on an as needed basis, approval maybe granted by the Medical Director for any access. Archiving of patient records is carried out periodically with secure storage in place at National Ambulance HQ.

Patient records – and other patient data information is kept within the Operations area in secured cabinets in locations where ePCR usage is not allowed for security reasons until the records are collected by logistics. The Chief Operations Officer is responsible for ensuring these files are secured on a daily basis. Archiving of patient records is carried out periodically with secure storage in place at National Ambulance HQ.

Dispatch records – is entered in the CAD system. Hard copies are only used when facing a CAD crash during which manual records are kept within the Operations area in secured cabinets. Data in the hard copy records is entered through the CAD once the crash is solved. The hard copies are then disposed of immediately. The Chief Operations Officer is responsible for ensuring these files are secure during CAD crashes. Accessing records maybe signed out by staff on an as needed basis, approval maybe granted by the Chief Operations Officer.

Vehicle records – Vehicle related records received as hard copies are filed in the respective ambulance folders in secure area in the National Ambulance Warehouse. The Fleet Manager is responsible for ensuring these files are secured on a daily basis. Soft copies of these records are maintained on OPIQ and are saved on N: Drive. Access to the Fleet Section of the N drive is only granted by the Chief Administrative Officer. Records maybe signed out by staff on an as needed basis, final approval is with the Fleet Manager for any access

Printed Copies and Reports- Printed Reports and printed copies of electronic records must be kept in accordance with the COP403 General Confidentiality Policy. Printed copies of electronic records should be disposed of according to COP402 Document Retention Policy & Procedure if the primary copy. Otherwise they should be disposed of when finished with.

Back Up – All data on the N: drive is backed up on a daily basis in accordance with ITP106 Data Back Up Policy. Physical records are kept in accordance with the COP402 Document Retention Policy & Procedure.

Admin Access – As part of the role of management and maintenance of data assets, IT, HR, Clinical Audit and Finance staff have access to some information assets in the National Ambulance environment. Abuse of this privileged access, excessive access for no valid reason, tampering or unauthorized alteration of records or unauthorized disclosure of information from any of these admin staff members will be considered gross misconduct and dealt with accordingly and any disclosure of patient information and violation of this policy may result in disciplinary action in accordance with COP102 Disciplinary Policy

4.11. Education of Staff

New staff are made aware of their responsibilities in relation to Information Management during their induction. Through the production of reports to the executive team this will allow staff the opportunity to :-

- Understand security and confidentiality of data and information
- Use measurement instruments, statistical tools and data analysis methods
- Assist in interpreting data
- Use data and information to help in decision making
- Educate and support the participation of patients and families in care processes and
- Use indicators to assess and improve care and work processes.

4.12. Aggregate Data and Information

Aggregate Date and Information support patient care, organization management and the quality management system. As the organization develops, it is vital that information be used in an effective manner over time and allows the comparison of National Ambulance's performance against other organizations.

Under the direction of the Medical Director, National Ambulance will share and monitor its aggregate data and information to develop and continuously improve operations and service delivery.

The Medical Director has the authority to release information that has been appropriately cleared of identifying factors. When sharing data the Medical Director is to report the release of the data to the Chief Executive Officer.

4.12.1. Data Validation

A data validation audit and impact assessment will be completed periodically by data owners to ensure the quality of key data for the organization. Ensuring validity and accuracy of data critical for creating correct improvement plans which eventually leads to effective decision making. Data validation must be completed when:

- A new measure is implemented
- Data will be made public upon request
- A change has been made to an existing measure
- The data resulting from an existing measure have changed in an unexplainable way
- The data source has changed

Data Validation Methodologies:

- Sample analysis: sample data taken from the source system validated against actual values.
- Source to source verification; data from two or more systems is compared and validated where disparities occur.
- Source system loop back verification: using aggregate data to track issues e.g. total values or total no. of calls per day
- Regression testing; running the same reports for the same periods both before and after changes to systems.

All the above methodologies must be used appropriately with the participation of appropriate stakeholders for full peer review. Recording of validation must be completed prior to any change going into production.

4.13. Removable Media

Use of removable media for the access and storage of confidential information is to be controlled and requires approval from the information owner as defined previously.

Removable media storing confidential information must be asset tagged, encrypted, and issued to an individual for safe keeping.

Responsibility for the loss or misuse of any data stored on removable media or USB sticks resides with the person to whom the removable media was issued. Accountability for the loss or misuse of confidential information stored on removable media resides with the information owner as defined previously.

IT will perform an audit to ensure removable media is still in the possession of the individuals issued the media as required.

Unused or removable media that is no longer required to store confidential information will be returned to IT for wiping and safe keeping.

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
Abu Dhabi Health Information Cyber Security standard (ADHICS)	Abu Dhabi
DoH Standard On Patient Healthcare Data Privacy	Abu Dhabi
Federal Law No. (1) Of 2006	UAE
Federal Law No. (2) of 2019	UAE

6. RELATED POLICIES AND FORMS

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

Policy & Procedure /Form
COP403 General Confidential Policy
COP402 Document Retention Policy & Procedure
QHP213 QHSE Work Location Management Policy
CGP119 Patient Care Record and Documentation Policy and Procedure
OPP113 Ambulance Communication Center Procedure
ITP125 IT Operations Policy
ITP101 Information Technology Policy
ITP106 Data Backup Policy
ITP121 Clear Desk and Clear Screen 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:

- Chief Executive Officer

Change Brief

Version No.	Date	Change
1	16-January-2014	New Document
2	29-May-2014	Migrated to Corporate
3	14-Jan-2016	Updated for JCI 2nd Edition
4	November 2017	Updated to include 998 call, CCTV and Biometric data access
5	November 2019	Add validate data to aim of policy, Replaced CMA with MD, Revised the Roles and Responsibilities, Updated 4.11 Protection of Records, Add 4.13.1 Data Validation, Add 4.6 Vehicle Records and 4.12 Protection of Records – Vehicle Records
6	September 2020	- Added CFO in roles and responsibilities - Added NDA - Added information classification criteria, protectively marking and identification of information assets, access control, confidential information assets, information systems governance and service ownership, access controls, and termination of access clause - Amended access to information and protection of records clause
7	April 2021	- changes in clauses 4.3.1 Information classification criteria and 4.3.2 Protectively Marking and Identification Of Information Assets - Addition of “and is responsible for the oversight and monitoring of clinical data confidentiality and privacy” in Medical Director roles and responsibilities. - ADHICS added to Public Classification Note: national ambulance is not obliged to label the public information assets as long as its stipulated in a policy - Added section on removable media and removed technical parts of claims process as should not be in a policy

CEO Approval

Board Member Verification