State of Qatar
MINISTRY OF PUBLIC HEALTH

Cancer Data Security Policy

Document Control Stamp

MINISTRY OF PUBLIC HEALTH
CONTROLLED

Approval:

MINISTRY OF PUBLIC HEALTH
PLANNING & QUALITY DEPARTMENT

Revision History

Revision No.	Reviewed by	Approved by	Effective Date	Remarks
00			16 FEB 2021	Initial release
	Mohammed Hamad J. Al-Thani	Dr. Salih Ali Al Marri		
	Director	Asst. Minister for Health Affairs		

1. Purpose

1.1 This policy aims to protect the sensitive patient data entrusted to it by data providers under direction of and by agreement with the Ministry of Public Health MoPH.

2. Policy Scope and Applicability

2.1 It is the intent of the Ministry of Public Health MoPH management to provide direction and an environment that facilitates the communication and use of information within the bounds of sound business practices, and the legal or regulatory restrictions that apply. Security policies, standards, procedures, and business continuation plans have been developed to provide consistency in implementing controls. These define protection requirements or provide guidance to management responsible for implementing controls within their business functions. It is the intent of this policy to facilitate the exchange of information and computing resources while balancing the need for protecting information with the cost of implementation functions and departments/sections/job titles this policy covers.

2.2 This policy contains a high-level statement of the Ministry of Public Health MoPH information security intentions, expectations, and objectives, and the necessary implementation strategy for their attainment. All information, data, applications, networks, and equipment (including computers and printers) are the property of the Ministry of Public Health MoPH and are provided to its employees so that they can conduct their job responsibilities effectively.

3. Definitions

3.1 None

4. Policy Statement

4.1 Information Assets: The Ministry of Public Health MoPH information and information processing infrastructure are essential assets requiring protection commensurate with their risk value. Organizational information, applications, systems, and networks must be actively managed to ensure security, confidentiality, integrity, and availability.

4.2 Accountability: The administrative and departmental computing environments will maintain consistent standards for establishing the accountability and authenticity of system users. These environments will develop unique standards for protecting information, applications, systems, and network resources contained within these environments that will be commensurate with fulfilling the mission of the Ministry of Public Health MoPH and maintaining the integrity of those critical resources.

To maintain accountability for system access, the following will be implemented:

- All individuals with access to the systems will use a user ID that has been specifically assigned to that individual. Sharing of user IDs is prohibited except in specific, approved situations. Written justification for such an ID is required and approval for use will be granted only by senior management.
- All individuals with network, system, and application user IDs will retain a confidential password that will be used to authenticate the identity of the individual. Intentional disclosure or sharing of passwords is prohibited. To meet the needs of some applications, certain terminals can utilize a location or station password, with strictly limited access to applications. User IDs will be required on all documents generated or modified.

4.3 Information Access: All access to information is to be authorized by responsible management, with access granted or revoked based on business requirements only. Access to administrative data will be granted to the Ministry of Public Health MoPH employees only. Individuals outside of the Ministry of Public Health MoPH can be authorized access to the Ministry of Public Health MoPH data only if that authorization is granted by the appropriate Department Manager and the IT Security.

Access and update capabilities/restrictions will apply to all the Ministry of Public Health MoPH administrative, departmental, and operational data, stored on their respective systems computing facilities. Security measures apply to all systems developed and/or maintained by the Ministry of Public Health MoPH locations, departments, organizations, affiliates, outside vendors, or contractors.

The appropriate Department Manager and the System Administrator are responsible for authorizing access to systems and information, verifying information integrity, and controlling extracted information. Management is responsible for developing secure processing systems and operating these systems in a controlled environment. Employees are required to comply with management's direction for the use and protection of information technology processing systems and information. Employees must be kept aware of the importance of information security. All managers and employees are required to act with urgency and diligence to fulfil these requirements.

Risks must be evaluated to determine the optimum level of control required for each type of information technology system. Adequate controls are to be included to ensure that information security, confidentiality, integrity, and availability are achieved.

4.4 Violation of Policy: Violation of this policy shall be brought to the immediate attention of the Security Office. Instances of known or suspected employee, either ethical or commercial infidelities, shall be reported to the Departmental Manager and the Security Office. The Security Office will work with Department Managers, System Administrators, and the Management

Team to ensure that the problem is resolved and to address necessary steps to eliminate future violations.

The Ministry of Public Health MoPH reserves the right to discipline, terminate, suspend, or prosecute, at its discretion, individuals who violate the Information Security Policy.

4.5 Risk management: Risk assessment involves identifying the sensitivity and criticality of information and the consequences to the Ministry of Public Health MoPH if information is disclosed, modified, or destroyed. Risk assessment techniques can include formal methods of determining the financial and operational impact of a security incident as well as less formal assessment techniques. A risk assessment process shall include the following elements:

A determination of the information assets that need to be protected.

Evaluation of the sensitivity of the information and the consequences if information is disclosed.

Evaluation of the criticality of information and the consequences to business processes if information and information processing systems are not available.

A determination by management of the extent of risk that will be accepted, mitigated, or transferred.

Development of a risk control strategy.

Determination of compliance with regulatory information classifications.

It is the responsibility of management to understand the level of risk to the Ministry of Public Health MoPH relating to the confidentiality, integrity, and availability of information and to the controls necessary to effectively mitigate this risk. Risk control measures shall address not only the information but the processes that are used to create, modify, report, or distribute information, and the environments under which these processes exist. This process shall also incorporate the classification of data/information into one of the following categories:

- Public
- Internal
- Confidential

5. Appendices

5.1 None

6. Related Documents

6.1 None