



Malaffi Security Assessment Guideline

SECURITY ASSESSMENT GUIDELINES

What is the Malaffi Security Assessment

- This assessment **does not replace** DOH's Abu Dhabi Health Care Information and Cyber Security Standards (ADHICS) compliance requirement.
- Healthcare facilities are required to submit their DOH ADHICS compliance status to DOH directly on a Quarterly basis to adhics@doh.gov.ae.
- The Malaffi Assessment is a set of 41 controls from ADHICS (a sub-set of ADHICS) related to key information security areas/domains ensuring the privacy and Security of patients healthcare information in Abu Dhabi. Passing these 41 controls is a minimum requirements in order to be able to connect to Malaffi.

SECURITY ASSESSMENT GUIDELINES

Process

Healthcare facilities are required to meet the minimum baseline standard requirements to be able to integrate with Malaffi. All Participants must complete the Malaffi Security Assessment (one per group of facilities who use identical security controls). In order to avoid any delay in your onboarding process, please ensure to fill in all cells in the Provider info and Evaluation tabs and forward your assessment/s to onboarding@malaffi.ae as per the deadlines given.

Once received, Malaffi will review the Security Assessment score/s, and together with the DOH, determine and notify the Providers on their status.

Status types:

- **Not approved:** Participants will not be allowed to exchange patient information through Malaffi. Participants will need to make rectifications to their current security standards and resubmit security assessment to Malaffi within the specified timeframe provided by the Malaffi Information Security Team.
- **Conditionally Approved:** This is a preliminary approval to proceed with the Malaffi connection with the expectation that the Participant will complete the required rectification as per the timeline given by the Malaffi Information Security Team.
- **Approved:** Malaffi can proceed with the connectivity of these Participants.

SECURITY ASSESSMENT GUIDELINES

Provider Info Tab

- Helpful comments within the cells
- All Fields are Mandatory

Provider Information		
<p>The purpose of the survey is to assist the ADHIE team in gathering initial information about your organization to assist with the implementation planning efforts. Please complete the survey based on information that reflects your organization as of today. If you have any questions reach out to ISO@malaffi.ae.</p> <p>Make sure you read the comments embeded within the excel for instructions.</p>		
Provider/Participant Name: List of Facility/ies DoH License nos. (MF or PF) WHO SHARE THE SAME ELECTRONIC HEALTH INFORMATION MANAGEMENT SYSTEM AND SECURITY POLICIES. (Please add rows if needed)	FACILITY LICENSE NO.	FACILITY NAME
If you have an electronic health information management system (i.e. - EMR, LIS or Similar?), what is the Type?		
Who is your electronic health information management system vendor?		
If you do not have an electronic health information management system, what is your projected timeline for implementing?		
Name of Person Responsible:		
Email Address of Person Responsible:		
Mobile Number of Person Responsible:		
Name of Chief Information Security Officer (CISO) / Chief Cyber Security Officer (CCSO) or similar:		
Email Address of CISO / CCSO or similar:		
Mobile Number of CISO / CCSO or similar:		
Submission Date		



SECURITY ASSESSMENT GUIDELINES

Evaluation tab

UOL MALAFFI

Evaluation Questionnaire

#	Domain	ADHICS Control	Security Control Questions	Response	Evidence (if fully compliant) / Justification (if not applicable)	Plans to be compliant (if partially compliant or non compliant)	Target date of Compliance
1	HR Security	HR 3.4	Are periodic security awareness campaigns established for the workforce?				
2	Physical and Environmental Security	PE 11	Have physical and environmental security policies been developed and implemented to ensure adequate physical and environmental protection of information assets?				
3	Access Control	AC 1	Have access control policies been developed and implemented to ensure appropriate access to information and information systems are adequately controlled and secured?				
4	Access Control	AC 2.1	Does a formal user registration and de-registration process exist?				
5	Access Control	AC 2.2	Are user accounts restricted and controlled based on principles of need to know?				
6	Access Control	AC 2.3	Are processes in place to ensure the secure allocation, use and management of security credentials? (i.e. default application passwords are changed and not used, passwords are always encrypted, strong)				
7	Access Control	AC 3.1	Are controls in place to protect confidential and secret information on portable or removable media and mobile devices?				
8	Access Control	AC 3.2	Are controls in place to manage access to equipment, devices, systems and facilities at teleworking sites?				
9	Access Control	AC 4	Are processes in place to review access and privileges granted to its users?				
10	Access Control	AC 5.1	Is access to your network and network services controlled and based on specific need for which the user is authorized for?				
11	Access Control	AC 5.2	Do secure controls exists for remote login? (i.e. IPsec VPN, Multifactor Authentication etc.)				
12	Access Control	AC 5.7, CM 5.4	Are controls in place to ensure wireless access is secured?				
13	Access Control	AC 5.7	Is public and guest access provided to the Wi-Fi network? If so, is it segregated from the internal network?				
14	Access Control	AC 5.7, CM 5.4	Are strong encryption mechanisms in place for all wireless connections?				
15	Access Control	AC 6.1	Are secure log-on and log-off procedures to control access to systems and applications enforced? (i.e. force automatic workstation lock and time-outs etc.)				
16	Access Control	AC 6.2	Are processes in place to ensure that all users have a unique identifier				

Entity Info Evaluation Evaluation Summary

Correspond directly with ADHICS control domain and requirements

Response: select appropriate response based on your current state.

Evidence: Only required if you respond Fully Compliant or Not Applicable. The evidence supplied must be sufficient to meet ADHICS guidelines.

Plans to be Compliant: Only required if you respond with Partially Compliant or Non Compliant. Hint: Document your partial controls and also what controls you plan to implement to become fully compliant

Target Date (DDMMYY): Required if you respond with Partially Compliant or Non Compliant. Hint: Your dates must be inline with the Onboarding plans.

SECURITY ASSESSMENT GUIDELINES

Evaluation Summary

FOR MALAFFI INTERNAL REPORTING PURPOSE ONLY. PLEASE DO NOT EDIT THIS WORKSHEET.

Security Assessment compliance score



Evaluation Summary

Overall Control Implementation #DIV/0!

No. of "Not Applicable" Controls 0

Response	Total
Fully Compliant	0
Partially Compliant	0
Non Compliant	0
Not Applicable	0
Total Applicable Controls	0

Compliance Status 0 0%

Fully Compliant
Partially Compliant
Non Compliant

Control Status	Definition
Fully Compliant	The control/sub-control is fully implemented, has been established and has a process, and is regularly updated.
Partially Compliant	The control/sub-control is implemented but not across all of the entity's information systems, and a process has not been fully established, or is outdated.
Non Compliant	The control/sub-control is not planned nor implemented.
Not Applicable	The control is not applicable.

Entity Info Evaluation Evaluation Summary

SECURITY ASSESSMENT GUIDELINES

Resources

- The controls are defined in the ABU DHABI HEALTHCARE INFORMATION AND CYBER SECURITY [ADHICS] Standard (DOH/SD/ADHICS/0.9), below:

<https://www.doh.gov.ae/-/media/B7BF46EC6D37426C883509CA66734EB4.ashx>

- The guidelines for implementation have been provided through ADHICS Implementation Guidelines (DOH/Guidelines/ADHICS/0.9), below:

<https://www.doh.gov.ae/-/media/E20D8A6D109E45579637151F75E61FD8.ashx>

- For Malaffi Security Assessment please contact iso@malaffi.ae.



The End