Please scan and email completed form to: servicedesk@sharedhealthmb.ca	*Incident #*	

Winnipeg Regional Health Authority / Office régional de la santé de Winnipeg — Caring for Health / À l'écoute de notre santé

Access Request Form for Personal and/or WRHA Affiliate Wireless Devices

NOTE: Only send one request form per email to Service Desk

Shared health Soins communs Manitoba

Part A	**DEVICE INFORMATION**	**DATE OF REQUEST:**	
Device Phone #:		Device Make:	
User's Email Address:		Device Model:	
*DEVICE ID**:			
	* To obtain the DEVICE ID, you must first set up your corporate email on your device using the instructions at: https://home.sharedhealthmb.ca/files/access-request-form-personal-wrha-affiliate.pdf - Once your email is set up, your DEVICE ID will be emailed to you from *Microsoft Outlook*.		

Part B	**USER INFORMATION**		
Organization Name:			
User's Name:	User's Title:	User's Contact #:	
Department:	Organization Address:		
Requester's Name: *(if different from user)*	Requester's Phone #:		

Part C	**RATIONALE FOR REMOTE NETWORK ACCESS**
As per WRHA Policy 10.20.025 all remote access requests must be pre-approved by the requester's Manager/Director.	
Rationale for request	

Part D	**APPROVAL SIGNATURE** *Approves requester's network access on a personal device.*
	Manager/ Site Director Approval
	Print:
	Date:
	Signature:

Part E	***INTERNAL USE ONLY***
Shared Health, ICT Client Services Director Approval	

Print:	*Date:*	*Signature:*

Please complete the form in its entirety.
Incomplete forms will be sent back to the requestor and will result in processing delays.

Revised: Apr. 15, 2019

NETWORK ACCESS COMPLIANCE STATEMENT

Note: **This form is intended for both corporate iPhones and personal devices.**

Please complete both approved documents when submitting to the Service Desk. Once the completed form has been received, you will be eligible to have your device connected to the WRHA network.

By signing my name below, I acknowledge and agree to the following:

1. I acknowledge the paramount importance of the security of the WRHA network and computer systems. I recognize that, in order to maintain that security, if a breach should be found originating from my device, network access for my device may be disabled without prior notification.
2. I pledge to follow WRHA policy and maintain a minimum password of **six (6) digits** on my device while Digital Health network access is maintained on it.
3. I will be allowed 10 password login attempts before my device is wiped.
4. While I have access to the WRHA network, my device will be restricted to a ten-minute timeout password lock.
5. Due to the nature of remote access technology, Digital Health will **not** assume end-to-end responsibility for the availability of network access on personally owned devices. Therefore:
    - Digital Health will **only** provide troubleshooting support for remote network access and will **not** support my personally owned hardware.
    - From time to time, security settings are subject to change. Digitial Health will make its best effort to inform me of the changes in a timely manner.
6. Without exception, my device will be governed by all WRHA policies, Digital Health standards and guidelines surrounding the protection of personal health information, personal information, corporate information and intellectual property.
7. I am responsible for notifying the Service Desk at 204-940-8500 if I no longer require network access on my device, if I upgrade my device or if I leave the organization.
8. I am responsible for regularly backing up my personal pictures/contacts. Digitial Health is not responsible for the retrieval of personal data (personal contacts/pictures).
9. I will not back up/copy corporate data to any storage solution. This includes but is not limited to personal computers, thumb drives or Cloud services.
10. In case of theft and/or loss of my device, I will immediately notify the Service Desk at 204- 940-8500 in order to disable network access to my device.
11. Digital Health will immediately wipe my device back to manufacturer state (including the wiping of personal pictures/personal data) in the event that my device is lost or stolen or in the case of employee dismissal from the WRHA.

12. Digital Health will proactively check the network activity of my device; if my device is found to be inactive for more than 90 days, it will be locked out from network access. I will contact the Service Desk if I require my device to be reconnected.
13. From time to time, I will be asked to re-enrol my device on the network. Digital Health will do its best to communicate this change as necessary.
14. On an annual basis, Digital Health will distribute a list of all end users with access to the network; each organization will be asked to validate existing users of this service.

POLICY REFERENCES:

Use of Portable Electronic Devices and Personal Computers Policy (WRHA Policy 10.20.025) Computer/

Internet Use Policy (WRHA Policy 70.20.010)

Information Technology Security Policy (WRHA Policy 70.30.010)

Wireless Local Area Network Technology (WRHA Policy 70.30.020)

I, as the intended user of remote access on my personal and/or corporate device, have read and understand the above statement.

Name: (print) _____ Signature: _____

Date (yyyy/mm/dd): _____

SITE MANAGER/DIRECTOR

Name: (print) Date _____ Signature: _____

(yyyy/mm/dd): _____

INTERNAL USE ONLY

Shared Health, ICT Client Services Director

Name: (print) _____ *Signature:* _____

Date (yyyy/mm/dd): _____