Physicians Working Remotely

Context

The COVID-19 pandemic changes the way physicians work. Some are required to self-isolate. All promote social distancing at clinics and facilities. Work needs to continue when remote from offices, clinics or facilities, with implications acknowledged by the College of Physicians and Surgeons of Alberta (CPSA) and others.

This guide offers practical advice about how physicians can work remotely while remaining mindful of organizational, legislative and professional obligations.

On our Best Behavior

Physicians performing tasks that would normally be occur in a health care facility should be heed the same privacy and security considerations that apply at the facility, including:

- Completion of mandated AHS Privacy and Security awareness training ("Infocare: On Our Best Behaviours") through MyLearningLink.
- Use of a dedicated work area where private conversations can be conducted.
- Use of computer device(s) that meet AHS hard encryption requirements for sensitive information.
- Adherence to strong password policies and automated inactivity logoffs to prevent uncontrolled access.
- Not saving or storing files bearing personal health information unless the remote venue has prepared and submitted a privacy impact assessment.
- Use of AHS-secured systems (e.g., SharePoint, clinical information systems) for protected file management.
- Use of secure communication technologies (including AHS secure email, clinical information system messaging, AHS teleconferencing) when communicating with providers or patients about healthcare.
- Capacity to securely destroy (manually or digitally shred) any temporarily rendered items bearing personal health information or identifiers.

AHS Credentials

Physicians seeking access to AHS information assets need AHS "HEALTHY" credentials. These are the username and password used to log on to AHS Windows devices in AHS facilities. The same credentials are used with AHS email accounts.

Normally, AHS credentials are provided at the time of physician on-boarding and privileging. This is handled through Zone Medical Affairs (see Connect Care Physician Manual – Remote Access for details). Medical Affairs should be contacted by AHS-affiliated physicians who believe they do not yet have AHS credentials.

AHS Remote Access

AHS HEALTHY credentials can be associated with one or more levels of access. Permission to use an AHS username/password for remote access (outside AHS facilities) is normally granted as part of physician on-boarding through Zone Medical Affairs. All eligible physicians are contacted and provided with information about how to activate this access, then use a security "FOB" to add a just-in-time security code to username and password at the time of remote access to sensitive resources.

Having remote access to Netcare (through Alberta Health) does not necessarily mean that remote access has been granted for AHS information tools.

Those who have failed to follow AHS remote access instructions at the time of on-boarding, or who feel they may have been missed, should contact Zone Medical Affairs. Remote access and security FOB instructions are provided in the Connect Care Physician Manual – Remote Access.

Remote Work Strategies

For providers with working AHS credentials and a working security FOB, three strategies for working remotely are supported. All assume that the physician might need:

- Productivity software (e.g., Microsoft Office),
- Communications tools (e.g., AHS secure email),
- Information stores (e.g., AHS Insite, AHS SharePoint, AHS Shared Drive, etc.), and
- Clinical applications (e.g., Connect Care, SCM, Meditech, Impax, etc.).

Option 1: Personal Computer – Personal Productivity Software – Citrix Workspace

This (preferred) remote work strategy is most commonly used by AHS physicians on personal devices.

- **Productivity** - personally licensed and maintained on a personal computing device,
- **Communications** – AHS email accessed via compatible email software (e.g., Outlook, Apple Mail, Thunderbird, etc.) or via WebMail (email.ahs.ca),
- **Shared information** – AHS username/password logon to insite.ahs.ca, share.ahs.ca and other resources,
- **Shared drives** – remote access (username/password/FOB) to myapps.ahs.ca then “Windows Explorer” app,
- **Clinical applications** – remote access (username/password/FOB) to myapps.ahs.ca then available clinical apps.

Remote work is done on a personal computing device (desktop, laptop, etc.) with the protections described. The user’s own instance of Microsoft Office, for example, is used (institutional pricing available through an AHS Home Use Program). AHS intranet (insite.ahs.ca) and email applications are accessed with the user’s AHS username and password while clinical applications and shared drives are accessed with username, password and FOB code via myapps.ahs.ca.

MyApps opens a “virtual machine” within which clinical and other AHS applications work. This requires installation of Citrix Workspace. Instructions, tip sheets and troubleshooting guides are provided in the Connect Care Physician Manual.

Option 2: AHS Computer – AHS Productivity Software – Virtual Private Network

Some physicians are assigned an AHS-provisioned computer that can be used in a remote setting.

- **Productivity** – AHS licensed and installed instance of Microsoft Office.
- **Communications** – AHS email accessed via Microsoft Outlook.
- **Shared information** – AHS VPN (username/password/FOB) for access to AHS Intranet assets
- **Clinical applications** – Direct or Citrix Workspace apps pre-installed and configured

The AHS computer will have been configured with software applications, including clinical ones, needed by the physician-user. It is not possible for the user to install additional software.

NetMotion is a Virtual Private Network (VPN) solution installed on AHS computers used offsite. It enables secure communication between a device (AHS laptop) and the AHS network. Once logged in through NetMotion (with AHS credentials and FOB security code), the experience is equivalent to using an AHS workstation onsite location. The installed Internet Browser (Internet Explorer) can be used to access insite.ahs.ca and myapps.ahs.ca.

IT Service Desk (1-877-311-4300) provides support for any needed NetMotion or other AHS computer configuration needs.

Requests for AHS devices are made through Zone Medical Affairs and are allocated based on administrative approval and demonstrated need.

Option 3: Remote Desktop Access to AHS Desktop Computer

This model can be tricky to implement and unreliable in practice. It assumes that the physician has a fully enabled AHS desktop computer that is permanently turned on and network-responsive within an AHS facility. The AHS desktop computer has “Remote Desktop” (Windows) host software installed.

When working offsite, the physician can use Remote Desktop (Windows) client software to open a “window” onto the AHS computer and interact with it from afar.

This option requires knowledge of the “asset number” of the AHS onsite computer, found on the computer’s AHS identity tag (number starting with M). This identifier must be included in an application to AHS IAM to take advantage of remote desktop access. Instructions will be provided via email, including how to install and configure Virtual Private Networking (VPN) software required for this option.

Note that videoconferencing tools, like Skype for Business, tend to malfunction in this model.

Clinical Tools

Using Citrix Workspace via myapps.ahs.ca is well described in the Connect Care Physician Manual, with supporting tip sheets.

Collaboration Tools

Physicians working remotely can continue to use Skype for Business or AHS Zoom to facilitate videoconferencing, web meetings, webinars or even virtual care; all as described in the Connect Care Physician Manual.

Printing

As much as possible, printing should be avoided when working remotely. Anything printed for temporary convenience should be shredded after use. If sensitive documents will be printed and retained, a secured workspace must be covered by a current Privacy Impact Assessment.

Some clinical applications may be configured to print to specific clinical locations, requiring care and work-arounds when printing remotely.

- Tip: Remote Printing in Connect Care

Resources

- Connect Care Physician Manual – Access
- Connect Care Physician Manual – Virtual Care
- AHS Information & Privacy Home Checklist
- AHS Options for Working from Home
- Accessing Your Applications Remotely