Primary Care Network
EDMONTON SOUTHSIDE

3110 Calgary Trail NW
Edmonton, AB T6J 6V4
Phone: 780.395.2626
Fax: 780.435.5526

FAQ: EMR Access Requirements for Proactive Care Coordination Assistants (PCCAs)

Q: What are the EMR login requirements for PCCA work?

A: PCCAs need an EMR login with access to template management/reports, and the ability to remotely access the EMR off site.

Q: What are the benefits to the PCCA working remotely?

A: Remote work ensures PCCAs have a private, quiet space where they can focus on their role and effectively interact with patients. PCCAs ensure optimal communication with clinic teams is maintained by using worklists and messaging tools embedded within the EMR. Remote work also allows PCCAS to support several clinics seamlessly on a rotational schedule. If they experience a technical issue at one clinic, or work has been completed mid-rotation, PCCAs may transition to support another clinic, maximizing their support for each clinic.

Q: Is there a cost?

A: The PCN pays for all equipment (ESPCN computer, extra monitor, soft phone app, headset) that is used for PCCA work, and the PCCAs do not require a clinic space to work. If a clinic's EMR license agreement requires an additional fee for new users, the ESPCN can also pay for the PCCA's initial EMR license, with clinics then being responsible for subsequent monthly fees associated with that account. Clinics receiving PCCA support have found the EMR license cost is negligible in relation to the revenue generated by appointments the PCCAs book, and cost of saved clinical time from the PCCAs updating certain chart information and calling patients.

Q: How are privacy standards met offsite?

A: The ESPCN is fully committed to meeting privacy standards. All ESPCN staff complete annual privacy training, including reviewing ESPCN organizational policies related to privacy, and the ESPCN Privacy and Security Manual. The ESPCN has Information Manager Agreements with all clinics and staff additionally may sign clinic-level confidentiality agreements. If you have any questions regarding our commitment to privacy, please let us know and we will connect you with our Chief Privacy Officer.

Q: How is information security maintained with remote access?

A: PCCAs have worked in over 80 clinics using remote EMR access and these clinics have never experienced a security breach from an ESPCN device. ESPCN devices will not connect to unsecured Wi-Fi networks and require an internet security level of Wi-Fi 6 to connect. ESPCN staff are also enrolled in mandatory cyber security awareness programs and annual training to ensure continued compliance with IT policies, best practices, and security methodologies. More information about our information technology security is available on the next page of this document.

ESPCN Information Technology Security

Technology Partnerships

We have established technology partnerships with premier Canadian and international technology providers to maintain a safe, secure, and authentic IT environment. We partner with a dedicated IT Managed Services provider for front-line and systems management support.

Our technology focus is on a securely managed "Cloud First" enterprise IT model with dedicated and proactive IT support services in place. We maintain both cloud and on-premises redundancies to ensure persistent network functionality, resiliency, and continuity (backup and restore protocols).

Advanced Protection

Our partners are committed to active IT Lifecycle Management arrangements to support and secure front-line users and ESPCN back-end technology architecture. Network resources are secured using industry-leading Perimeter Security Services (Firewall) including Intrusion Prevention/Intrusion Detection Services (IPS/IDS) and reputation enabled defences. We also use layered Multi-Factor Authentication (MFA) and Advanced Endpoint Protection (AEP) services to prevent, detect, and mitigate endpoint-directed cyber threats.

Cloud resources are secured through technologies that include Transport Layer Security (TLS), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES). Data managed by the ESPCN is encrypted at rest and in transit, using strong encryption protocols.

Compliance and Standardization

We maintain compliance to technology-focused privacy and security requirements through adherence to cybersecurity frameworks, protocols, and best practices. Technology partners that furnish our health information services follow the Health Information Act (HIA) requirements to maintain privacy controls and compliance.

We require our primary IT Managed Services partner to maintain Service Organization Control (SOC2) cybersecurity compliance and a CyberSecure Canada (National Standard CAN/CIOSC 104:2021) certification. Adherence to ISO/IEC 27000:2018 IT security control standards and NIST cybersecurity standards is also required.

Questions?

If you have any technical questions regarding ESPCN account security, please let us know and we will connect you with our Technical Account Manager.