Vancouver Division of Family Practice
Security & Technology Assessment

Sample Medical Clinic

Performed by Andy Wynden and Roshan Shetty
with Dr. [Doctor Name] and [MOA Name] (MOA, IT Lead) on Sept 1, 2024

Assessment Summary

EMR Security	Adequate
PC Security	Adequate
Network Security	Robust
Physical Security	Robust
Vulnerability Awareness & Planning	Adequate
Data Security & Integrity	Needs improvement

The range of possible assessments are ‘Needs improvement’, ‘Adequate’, and ‘Robust’.

Preface

It was a delight to have an opportunity to discuss Sample Medical Clinic’s cybersecurity with both of you, and to discover how many best practices are already in place. We were delighted to see how invested you both are in your overall clinic security, as well as having had the opportunity to gather your excellent feedback regarding provincial systems and bugs you have encountered.

If you have any questions, feedback, or would like some support in implementing some of these recommendations, please do not hesitate to reach out either Andy or Roshan.

Andy Wynden
Tech Concierge
Vancouver Division of Family Practice
(250) 884-0797 (phone)
concierge@vancouverdivision.com

Roshan Shetty
Tech Concierge
Vancouver Division of Family Practice
(236) 862-6725 (phone or text)
rshetty@vancouverdivision.com

EMR Security

Summary

Your clinic's EMR security is adequate. Consider enabling IP restrictions and disabling concurrent sessions, as well as putting into practice a weekly or bi-weekly review of your clinic's audit logs so that any unauthorized access is noticed promptly.

Recommendation	Priority Level
Set password expiry policy	Medium
Disable concurrent sessions	Medium
Enable IP restrictions	Low
Review audit logs regularly	Low
Disable inactive accounts	Already in place
No shared accounts	Already in place
Avoid use of administrator accounts	Already in place
Avoid shared or re-used passwords	Already in place
Audit trails enabled	Already in place
Passwords meet minimum complexity requirements	Already in place
Passwords not saved in browser	Already in place

Detailed Recommendations

Set password expiry policy – medium priority

The CareConnect Privacy and Security Declaration signed by your site Privacy Officer during enrolment requires that passwords are changed at a minimum every 6 months. This is to ensure that anyone who has gained unauthorized access to an account's login credentials is not able to continue to access records indefinitely**. Consider setting an expiry date for all users' passwords to ensure compliance and to improve security.**

Guide to setting expiry dates for passwords in Oscar

Vulnerability Awareness & Planning

Summary

Overall, your clinic's vulnerability awareness & planning profile is adequate. We commend you for already having security policies and guidelines in place; that is a critical part of ensuring that every member of your staff understands their role in protecting your clinic from security or privacy breaches. Consider implementing annual or semi-annual cybersecurity training for your staff.

Recommendation	Priority Level
Regular staff cybersecurity and phishing training	High
Keep a record of all technical activities within the past 2 years	Medium
Review and update your clinic-wide security policy	Low
Review and update your clinic Incident Response Plan (IRP)	Low
Clinic-wide security policy communicated to all staff	Already in place
Clinic Incident Response Plan (IRP) communicated to all staff	Already in place

Detailed Recommendations

Regular staff cybersecurity and phishing training – high priority

A critical part of any business' success in security is staff training and awareness, as humans are the largest security vulnerability in any system. The CareConnect Privacy and Security Declaration requires security awareness training to be provided when onboarding new staff, as well as reviewed yearly. **Consider developing a policy to ensure this training is included in the onboarding process and reviewed on a yearly basis as part of your usual staff professional development.**

There is a list of resources in Appendix A of this report to help you create and source cybersecurity training for you and your staff.