Health Care Home Telehealth Module Technical Considerations Guide

A. NZ Telehealth Guideline for establishing & maintaining sustainable telemedicine services in New Zealand- Section 3, pg.4-5

https://www.telehealth.org.nz/assets/getting-started/Telemedicine-Guideline-for-NZTRC.pdf

B. Cybersecurity advisory regarding the implementation of telework and telehealth

www. patientsfirst.org.nz

Summary

Coronavirus Disease 2019 (COVID-19) will force many healthcare organisations to consider remote workplace options for their employees (VPN), new ways to interact with their patients (telehealth) and third-party communication (video conferencing/file share).

Some options can be secure when implemented properly, though if implemented in a rush or not properly maintained, may pose a significant risk.

Patients First recommends healthcare organisations explicitly anticipate and mitigate the cybersecurity risks around the use of telework and telehealth solutions.

Technical

The following are cybersecurity considerations regarding telework and telehealth in the context of COVID-19.

- As more organisations use VPNs for telework, increased cyber-risk arises out of targeting by malicious cyber actors.
- As VPNs are 24/7, organizations must keep them updated with the latest security updates and patches.
- Malicious cyber actors may increase phishing emails targeting teleworkers to steal their usernames and passwords.
- Organisations that do not use multi-factor authentication (MFA) for remote access are more susceptible to phishing attacks.
- Organisations may have a limited number of VPN connections, after which point no other employee can telework. With decreased availability, critical business operations may suffer, including IT security personnel's ability to perform cybersecurity tasks.

Recently impacted organisations and news:

- COVID-19 Testing Center Hit By Cyberattack
- New Ransomware Campaign Distributes CoronaVirus Ransomware and Kpot Infostealer
- Coronavirus Phishing Attacks Are Actively Targeting the US
- Fake Online Coronavirus Map Delivers Well-known Malware
- TrickBot Malware Targets Italy in Fake WHO Coronavirus Emails
- Practices urged to use standards-based telehealth platforms

Mitigations

Patients First recommends the following mitigating actions.

- Update VPNs, network infrastructure devices, and devices to remote into work environments with the latest software patches and security configurations. See CISA Tips Understanding Patches and Securing Network Infrastructure Devices.
- Alert employees to an expected increase in phishing attempts. See CISA Tip Avoiding Social Engineering and Phishing Attacks.
- Ensure IT security personnel ramp up key remote access cybersecurity tasks i.e. log review, attack detection, and incident response and recovery and review the *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.*
- Implement MFA on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords. (See CISA Tips Choosing and Protecting Passwords and Supplementing Passwords for more information.)
- Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications—such as rate limiting—to prioritise users that will require higher bandwidths.

Lastly, Patients First and our cybersecurity partner Medical IT Advisors can advise and respond to cybersecurity incidents, phishing, malware, and other cybersecurity concerns that may disrupt healthcare delivery during this global emergency.

References

CISA Insights: Risk Management for Novel Coronavirus (COVID-19)
CISA VPN Alert
National Security Agency Cybersecurity Advisory: Mitigating Recent VPN Vulnerabilities
Telework.gov Guidance
NZ Telehealth Resource Centre
Patients First
Medical IT Advisors

C. Cybersecurity 11 Top Tips:

- *Back-up your data*
- *Keep your devices and apps up-to-date*
- *Choose unique passwords*
- *Turn on two factor authentication*
- *Be creative with the answers to your account security questions*
- *Avoid sensitive transactions on free WiFi*
- *Install an antivirus and scan for viruses regularly*
- *Be smart about social media*
- *Limit the personal information you give on-line*
- *Check your bank statements*
- *Get a credit check*

These are not limited to Telehealth but business in general.

For full explanations of each tip go to:
https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/get-started-cyber-security/

For a visual guide:
https://www.cert.govt.nz/assets/Uploads/Infographics/Infographic-11-top-tips-for-cyber-security-A3.pdf