Infrastructure & Application Penetration Test
MetroCaring Health

Version: 1.0

Author: Ailsa Johns

28 February 2026

Document control

Document template

Document status	Version no.	Date	Author	Section / nature of change
Draft	0.1	-	Ailsa Johns	First issue
Baselined	1.0	28/02/2026	Ailsa Johns	Baselined template

Document change history

Document status	Version no.	Date	Author (optional)	Section / nature of change
Draft	0.1	06/02/2026	Ailsa Johns	Initial draft from generic template
Draft	0.2	07/02/2026	Ailsa Johns	Test details added
Draft	0.3	07/02/2026	Ailsa Johns	Summary completed, sent for internal review
Draft	0.4	14/02/2026	Ailsa Johns	Minor updates following internal feedback
Draft	0.5	15/02/2026	Ailsa Johns	Sent for initial customer review
Draft	0.6	27/02/2026	Ailsa Johns	Minor updates following customer review
Baselined	1.0	28/02/2026	Ailsa Johns	Baselined following customer review

Related documents

Document	Location	Status
Penetration Test Scope	Shared drive	Baselined
Certificate of Authority	Shared drive and appendix 1 below	Baselined
Penetration Test Remediation Plan	Shared drive	Draft

Document classification

Due to the nature of the information held in this document it has been classified by MetroCaring Health as **OFFICIAL-SENSITIVE** and should be processed in accordance with MetroCaring Health's **OFFICIAL-SENSITIVE** document guidelines.

Contents

1. Management summary

Security4Me Limited is pleased to present the findings of the recent infrastructure penetration test conducted for MetroCaring Health.

1.1 Overview and scope

Security4Me Limited was contracted by MetroCaring Health to conduct a penetration test of the company's infrastructure in accordance with the agreed penetration test scope. The reason for the testing was to identify whether MetroCaring Health's systems, and consequently its business reputation, could be compromised if an unknown issue led to data loss and / or system compromise. As the clinic will be operating via a hybrid infrastructure, security is paramount.

The tests were performed between 06/02/2026 and 28/02/2026 and carried out by Ailsa Johns.

The testing included:

- workstation / laptop review
- server review
- printer review
- social engineering review.

The IP addresses / IP ranges within this test were as follows:

Workstations / laptops

- 192.168.220.100 – 192.168.220.244 (dynamic host configuration protocol (DHCP)).

Servers

- Server01: 192.168.220.10 (Static)
- VoIP_Server: 192.168.220.16 (Static).

1.2 Caveats

As the systems in question were part of a live infrastructure and the testing was carried out during business hours, checks that would have an elevated risk of causing disruption were excluded. Denial of service (DoS) and distributed denial of service (DDoS) were excluded for the same reason, and these will be addressed in a separate test which will be conducted during an agreed period outside of working hours.

1.3 Risk ratings

Security4Me Limited has adopted the Common Vulnerability Scoring System (CVSS). CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritise responses and resources according to threat.

It should be noted that the score Security4Me Limited will assign is based upon the risk from a technical standpoint, assessing the overall business impact of any risk found is the responsibility of MetroCaring Health and falls outside the scope of this penetration testing.

Not all vulnerabilities fall within the scope of CVSS and where this is the case they will be highlighted as 'Custom' and assigned a risk severity of critical, high, medium, low or information, with notes on the reasons for the rating.

The table below gives a key to the icons used in this report to identify risk severity:

Symbol	Risk rating	CVSSv2 score range	Explanation
	CRITICAL	9.0 to 10.0	A vulnerability has been discovered that is rated as **CRITICAL**. This could mean that the system may be exposed to a known exploit allowing catastrophic damage / data breach. MetroCaring Health has advised that these issues need immediate resolution in < 2 days.
	HIGH	7.0 to 8.9	A vulnerability has been discovered that is rated as **HIGH**. This could mean that the system has known vulnerabilities which could expose the associated system allowing unauthorised access. This requires a resolution in the short term and MetroCaring Health has agreed that these issues need to be resolved in < 7 days.
	MEDIUM	4.0 to 6.9	A vulnerability has been discovered that is rated as **MEDIUM**. This could mean that the system has known medium level vulnerabilities linked to maintenance such as missing security patches. MetroCaring Health has advised that these issues should be addressed as part of the next maintenance cycle, for example, system patch updates.
	LOW	1.0 to 3.9	A vulnerability has been discovered that is rated as **LOW**. This could mean that the system has known low level vulnerabilities linked to maintenance such as missing security patches. MetroCaring Health has advised that these issues should be addressed as part of the next maintenance cycle, for example, system patch updates.
	INFO	0 to 0.99	A vulnerability has been discovered that is rated as **INFORMATIONAL**. This could mean that the system is not following best practice and should be reviewed for appropriate action.

1.4 Summary of findings

The following table summarises the risks found during the test:

Area	Critical	High	Medium	Low	Total
Workstations	1	1			2
Laptops	1		1		2
Servers	2	1			3
Mobile devices		1	1		2
Social engineering		1			1
Totals:	**4**	**4**	**2**	**0**	**10**

Note: the above figures do not include informational issues as these are not deemed an immediate threat.

The following table summarises the actions required to resolve risks identified:

Area	Risks
Workstations / laptops	4
Servers	4
Mobile devices	2
Social engineering	3
Total:	**13**

1.4.1 Key findings

The following summary shows the key findings for each area of the test:

1.4.2 Workstation review

Area:	Workstations	Overall risk rating:	Critical
There are four missing security patches that should be updated on all workstations as soon as possible.			

Area:	Workstations	Overall risk rating:	High
Default admin credentials used on telehealth workstations.			

1.4.3 Laptop review

Area:	Laptops	Overall risk rating:	Critical
There are two missing security patches that should be updated on all laptops as soon as possible.			

Area:	Laptops	Overall risk rating:	Medium
Unencrypted local storage of consultation notes.			

1.4.4 Server review

Area:	Servers	Overall risk rating:	Critical
VoIP server lacks disk encryption and non-compliance with UK GDPR.			

Area:	Servers	Overall risk rating:	Critical
There are three missing updates and two missing security updates.			

Area:	Servers	Overall risk rating:	High
VoIP server uses outdated TLS 1.0 for communications.			

1.4.5 Mobile devices

Area:	Mobile devices	Overall risk rating:	Medium
No authentication required when accessing confidential systems from the device.			

Area:	Mobile devices	Overall risk rating:	High
Mobile devices lack biometric authentication and no remote wipe capabilities.			

1.4.6 Social engineering

Area:	Workstations & social engineering	Overall risk rating:	High
Several employees failed simulated phishing attacks (for example, fake "IT department" emails) which would grant access to company workstations.			

1.5 Conclusion

1.5.1 Workstation / laptop review

The telehealth workstations reviewed were missing four high-risk operating system (OS) security patches, exposing patient data to ransomware risks. Workstations were also found with default administrator credentials on telehealth systems. Laptops were missing two high-risk OS security patches, and unencrypted local storage of consultation notes was identified.

1.5.2 Server review

Both servers have three missing updates and two missing security patches, exposing a risk to company systems. The VoIP server lacked disk encryption, violating UK GDPR requirements. The server was also found to be using outdated TLS 1.0 for telehealth consultations. These vulnerabilities risk the confidentiality and integrity of sensitive health data.

1.5.3 Mobile device review

Two significant vulnerabilities were identified in mobile endpoints. Mobile devices required no authentication when accessing confidential systems and were configured without biometric authentication or remote wipe capabilities, violating UK GDPR requirements for healthcare data protection.

1.5.4 Social engineering review

Several employees failed simulated phishing attacks, disclosing passwords or installing unverified software. Immediate retraining is required for affected employees, with emphasis on UK GDPR compliance for remote access to sensitive health records.

1.5.5 Next steps

1.5.5.1 Immediate / short term

- apply security patches to all workstations, laptops and servers to address vulnerabilities
- update admin credentials on telehealth systems
- enable BitLocker encryption on remote laptops to protect patient data from theft or loss
- enable encryption on VoIP server to protect calls and credentials from eavesdropping or tampering
- upgrade the VoIP server to use TLS 1.3 for secure telehealth communications
- enforce server-side authentication for confidential systems
- enforce biometric authentication and remote wipe capabilities on all mobile devices to comply with UK GDPR
- all staff to complete mandatory social engineering training session.

1.5.5.2 Medium / long term

- implement mobile device management (MDM) software to enforce security policies (for example, automatic updates, app whitelisting) on laptops and mobile devices
- conduct quarterly encryption compliance audits for remote laptops and mobile devices
- all staff to be trained on IT security, with an emphasis on remote working
- annual mandatory training provided on social engineering including, phishing prevention and data handling under UK GDPR
- integrate multi-factor authentication (MFA) for access to systems.

2. Detailed findings

The following sections give a detailed technical view of each issue encountered including any commands / tools used along with the tools output. They also contain recommendations to resolve any vulnerabilities found.

2.1 Generic notes

MetroCaring Health's hybrid infrastructure includes:

- 14 devices: 10 in-house (workstations) and 4 remote laptops, all DHCP assigned
- 2 servers and 1 printer:
  - Server01 (192.168.220.10): hosts patient records (GDPR-critical) and system backups
  - VoIP_Server (192.168.220.16): supports telehealth consultations
  - Printer01 (192.168.220.35): shared office printing service
- network core infrastructure includes 2 switches and 1 router:
  - Switch01 (192.168.220.30)
  - Switch02 (192.168.220.31)
  - Router01 (192.168.220.1)
- 4 mobile devices: assigned DHCP via internal network.

Excluded from testing: operationally critical services, including server infrastructure, DNS and DHCP, to avoid disruption. Separate auditing will be conducted.

2.2 Detailed workstation review

Workstations / laptops

We were not allowed to have a user login for the workstations so asked the IT Department to provide a list of patch levels for all users. The IT Department confirmed that:

- all workstations were created from the same image
- all laptops were created from the same image
- standard software installed includes telehealth tools (for example, Microsoft Teams, EHR access) in addition to Office 365
- all patch management is managed via a central WSUS server with patches released manually
- mobile device management (MDM) policies are not enforced for telehealth laptops
- all workstations and servers have their time set with an on-site Stratum 1 NTP server.

Patch levels

As no credentials were supplied for the Windows 11 clients, Security4Me Limited asked the IT Department to provide a list of all Windows 11 patches that had been applied to the workstations. The following critical patches seem to be missing:

Risk Rating: Critical
Risk Score: 9.1
Remediation Required: within 2 days

Workstations

2026-02 Cumulative Update Preview for Windows 11 Version 23H2 for arm64-based Systems	Critical Updates	03/02/2025
2026-01 Dynamic Update for Windows 11 for ARM64-based Systems	Critical Updates	01/01/2026

2026-01 Dynamic Update for Windows 11 for x64-based Systems	Critical Updates	01/01/2026
2025-11 Cumulative Update Preview for Windows 11 Version 22H2 for x64-based Systems	Critical Updates	11/11/2025

Laptops

2026-02 Cumulative Update Preview for Windows 11 Version 23H2 for arm64-based Systems	Critical Updates	03/02/2025
2026-01 Dynamic Update for Windows 11 for ARM64-based Systems	Critical Updates	01/01/2026

Recommended actions

1. The above patches are downloaded, tested and if OK applied to the workstations as a matter of urgency
2. As the workstation patching is manually distributed via WSUS, it is recommended that the patch management process including WSUS are revised to ensure patches are applied in a timely manner
3. Admin credentials are updated for telehealth workstations and password policy updated to ensure secure passwords for all systems and devices
4. BitLocker implemented for all remote devices using local storage of sensitive data.

Social engineering vulnerability test

Risk Rating: ⛔ High
Risk Score: 8.1
Remediation Required: within 7 days

As the workforce mainly work from the clinic, with some employees occasionally using laptops remotely, it was most appropriate to test all users.

The test involved contacting all users to ask them a series of questions to determine whether access could be gained to their device.

The questions were asked via telephone and the security representative from Security4Me Limited posed as the IT department responsible for all clinics, they included:

1. 'I urgently need to run an update on your computer remotely, could you please confirm your username and password as these will be updated to our new system as part of the update'
2. 'Please download the following software to your device XXXXXXXXX, as this will allow me to run security updates'
3. 'I will email you a link now, can you click on the link and then log into the page'

With these three questions, we can determine whether the respondent would disclose their password (all employees are informed no one should ever ask for their password) or would they allow a non-verified individual to direct them to download software, which could be loaded with viruses, remote access software or other information harmful to the company.

The results:

Question 1: a few respondents disclosed passwords, some respondents declined, most respondents asked for verification of identity and declined to allow access.

Question 2: some respondents followed the steps to download the software; most respondents did not allow the software download.

Question 3: some respondents clicked on the email link and logged in; some respondents clicked the link but didn't enter their login details; most respondents did not click the link.

Note: only a few respondents reported any suspicious behaviour to the IT Department following these questions.

This shows that there is a vulnerability in the decision making of employees assuming that they are speaking to a genuine representative of IT, and as such this circumvents all security measures and safeguards currently in place.

Recommended actions

1. All staff to be retrained on IT security
2. Annual mandatory training provided on social engineering
3. Staff involved in the vulnerability test to be provided with immediate remedial training.

2.3 Detailed server review

Server build review

There are two Windows 2019 servers with host names of Server01 and VoIP_Server with IP addresses as follows:

- Server01 – 192.168.220.10
- VoIP_Server – 192.168.220.16

Patch levels

As no credentials were supplied for the Windows servers, Security4Me Limited asked the IT department to provide a list of all Windows Server 2019 patches that had been applied to all servers. The following critical and security patches seem to be missing:

Risk Rating: Critical
Risk Score: 9.1
Remediation Required: within 2 days

2025-11 Cumulative Update Preview for Windows Server 2019 for x64-based Systems	Critical Updates	11/11/2025
2025-11 Cumulative Update for Windows Server 2019 for x64-based Systems	Critical Updates	11/11/2025
2026-02 Cumulative Update Preview for Windows Server 2019 for x64-based Systems	Critical Updates	12/02/2026
2026-02 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows Server 2019 for x64	Security Updates	13/02/2026
2026-02 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64	Security Updates	13/02/2026

Recommended actions

1. The above patches are downloaded, tested and if OK applied to the server as soon as possible
2. As the servers seems to have missed patching it is either missing from patch management or patch management is not centralised
3. If patch management is available all servers should be added and updated
4. If a patch management system is not deployed, consideration should be given to deploying an in-built Windows solution such as WSUS which is a free-to-deploy service for managing updates.

2.4 Detailed mobile device review

Mobile device
Risk Rating: ⛔ High Risk Score: 8.2 Remediation Required: within 7 days **Findings:** • No authentication is required from mobile devices when employees use them to access critical systems containing sensitive data • No biometric authentication or remote wipe functionality. This may be partly caused by these devices running outdated OS versions (Android 10). **Recommended actions** **1.** Enforce server-side authentication for confidential systems to secure access from remote devices **2.** Enforce biometric authentication on all mobile devices and enable remote wipe in the event a device is lost / stolen to comply with UK GDPR.