The Password Was 1234

What a single security assessment revealed about risks facing dental practices in South Africa — and why changing one password won't fix it

David Sykes[1]

A dental practice hired me to test the security of their network. What I found wasn't a sophisticated vulnerability or an obscure configuration flaw — it was something far worse, precisely because of how simple it was.

Buried in the practice management system was a support account created by the software vendor. It had been configured with full administrative privileges — unrestricted access to every patient record, every ID number, every clinical note and financial transaction the system had ever stored. The account existed so the vendor's technicians could log in remotely without having to request credentials from the practice each time.

- The password on that account was 1234.
- The practice owner had no knowledge it was there.

From the vendor's perspective, the logic was perfectly reasonable: build in a persistent support account so technicians can access the system remotely without chasing the client for login details every time something needs fixing. Efficient. Practical. The problem is what that logic actually produced — an undisclosed account with unrestricted administrative access, protected by a four-digit password that the practice owner didn't set, didn't know about, and had never been asked to change. Unintentionally, the well-meaning vendor had prioritised their own convenience over the security of every patient record in the system.

But the password wasn't the real problem.

If the story ended there — with a changed password and a stern word to the vendor — it would be a cautionary anecdote and nothing more. But the password was only the most visible problem. It was the unlocked front door. What lay behind it was an entire building with no walls.

That same assessment revealed a practice network with no segmentation whatsoever. The front-desk PC used for checking email and browsing the web sat on the same network as the server holding every patient record. A single phishing email opened by a receptionist could have given an attacker a direct path to the clinical database. There was no barrier between the two — not a firewall, not a VLAN, not even a basic access control list. In network security terms, the architecture was completely flat.

The practice management server was running an operating system that had not been patched in over two years. Known vulnerabilities — the kind published in security bulletins, catalogued, and actively exploited by criminal groups — were sitting in that system, waiting. The vendor's password may have been the easiest way in, but it was far from the only one.

Remote desktop was enabled and exposed directly to the internet, with no multi-factor authentication, no IP restriction, and no rate limiting on failed login attempts. Automated

[1] Dr David Sykes, BDS(Wits)
Private practice, Umhlanga, KwaZulu-Natal
Dr Sykes holds a CompTIA PenTest+ certification in cybersecurity and is the founder of WhiteHat4Hire, a cybersecurity consultancy focused on protecting dental, medical, and healthcare practices in South Africa.
Contact: whitehat4hire.com

scanners find services like these within hours of them going live. Brute-force attacks against exposed remote desktops are so common that they barely register as noteworthy in the security community anymore — they are "background noise", constant and indiscriminate.

Staff across the practice, and the dentist, were using the same login credentials for the practice management system. No one had ever been asked to use a unique password. Multi-factor authentication — the single most effective control against stolen credentials — had never been enabled on any system.

And the imaging equipment — the X-ray unit— was running on software so old it had passed end-of-life support. No patches. No updates. No vendor standing behind it. These devices were connected to the same flat network as everything else.

None of this was unusual. In fact, it was entirely typical. This is what the inside of most dental practice networks looks like. The password was simply the detail dramatic enough to make someone pay attention.

This is not a rare edge case.

South Africa is one of the most targeted countries in the world for cybercrime. According to Interpol's Africa Cyberthreat Assessment, South Africa ranks among the top three most cyberattacked nations on the continent, with healthcare identified as a priority target. The reason is simple: healthcare practices hold highly sensitive personal information — exactly the kind that commands premium prices on criminal marketplaces — and they are chronically under-protected.

Dental practices are not exempt. In fact, they represent an ideal target: small enough to lack dedicated IT staff, large enough to hold valuable patient data, and busy enough that the owners have neither the time nor the inclination to think about what is quietly accumulating in their server room.

"It's always worked before."

I understand the mindset. I am a dentist. I have thirteen years of clinical practice. I know exactly what the working day looks like — patients from seven-thirty, a lunch break that isn't really a lunch break, admin piling up, and a practice management system that has hummed along quietly in the background for years without ever demanding attention.

That quiet is not safety. That quiet is luck. And in cybersecurity, luck has an expiry date.

The threat landscape has changed fundamentally. Ransomware-as-a-Service now allows criminal groups to licence attack tools the way a dentist leases a Planmeca unit. The technical barrier to executing a sophisticated attack on a small medical practice has dropped to near zero. And unlike the thief who breaks into your rooms for the petty cash, a ransomware operator will encrypt every file on your network — patient records, X-rays, billing history, clinical notes — and demand payment before you can access any of it.

There are no degrees of ransomware.

This is the part most people don't fully appreciate until it happens to them. Ransomware is binary. You are either hit, or you are not. There is no partial infection, no minor inconvenience, no situation where you lose a few files but keep the rest. When ransomware executes on your network, it encrypts everything — and it does so within minutes.

If you are not prepared, your options at that point are genuinely terrible: pay a criminal organisation with no guarantee of receiving a working decryption key, attempt a technical recovery that may cost more than the ransom and still fail, or accept that years of patient data are gone. Practices have closed their doors permanently after ransomware attacks. It is not hyperbole — it is documented.

But here is the critical truth that changes everything: if you had prepared before the attack, the story ends differently. A properly configured, tested, and isolated backup means that when the encryption runs — and if you're unprotected, it's when, not if — you restore the backup, rebuild the system, and you're back seeing patients. The criminal gets nothing. The ransom demand is irrelevant. The attack fails.

That single measure — a real, tested, offline backup — is the difference between a catastrophic business-ending event and an inconvenient afternoon.

POPIA does not care how busy you are.

The Protection of Personal Information Act is now fully in force. As a dental practice owner, you are a responsible party under the Act — meaning you carry a legal obligation to implement appropriate technical measures to protect the personal information you hold. Section 19 is explicit: reasonable security safeguards must be in place.

A vendor password that has never been changed is not a reasonable security safeguard. But neither is an unpatched server, a flat network, an unmonitored remote access point, or a system where every staff member shares the same credentials. Each of these failures independently constitutes a gap in the standard of care the Act demands.

If your practice suffers a breach and the Information Regulator investigates, "I didn't know" is not a legal defence. And if patient data is exposed, you face the obligation to

notify those patients — every one of them — and potentially the Regulator as well.

You cannot fix what you have not found.

This is the lesson the "1234" password really teaches. The practice owner was a careful, conscientious clinician. He ran a good practice. He had not been negligent in any obvious way. But he had no idea what was running on his own network, because he had never had anyone look.

That is the uncomfortable truth about cybersecurity in healthcare: the most dangerous vulnerabilities are the ones you don't know exist. You can change every password you are aware of, and it will not touch the service accounts the vendor created without telling you. You can install antivirus software, and it will not segment your network. You can back up your data, and it will not close the remote desktop port that is visible to every scanner on the internet.

These are not problems that respond to a checklist. They are problems that require someone qualified to examine your systems, identify the exposures, and tell you what you are actually dealing with. A security assessment is the clinical equivalent of taking a proper history and doing an examination before you pick up the handpiece. You would never treat a patient without one. Your network deserves the same discipline.

Proactive or reactive — you will choose one.

In cybersecurity, you do not get to be neutral. Every day that a vulnerable system runs unaddressed is a day the exposure grows. The only real choice is whether you address it before an attacker does, or after.

The practice in my story was lucky. I was the one who found the open door, not a criminal. But the password was only the beginning. The assessment uncovered an entire posture that needed rebuilding — network architecture, access controls, patching cycles, backup strategy, staff awareness. The work that followed was not a single afternoon's fix. It was a structured process, guided by what the assessment revealed, to bring that practice to a defensible standard.

Most practices will not get the kind of warning this one did. Most will not discover the problem until it becomes an incident. And by then, the options are limited, the costs are high, and the damage — to the practice, to the patients, and to the trust that holds both together — is already done.

Don't wait for the incident. Find out what's on your network.

References

1. INTERPOL. African Cyberthreat Assessment Report 2025, 4th edition. Lyon: INTERPOL African Joint Operation against Cybercrime (AFJOC); 2025. Available from: https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

2. Wood Ranch Medical. Notice of ransomware attack and permanent closure. Simi Valley, CA; 2019. Reported in: SecurityWeek, 10 October 2019. Available from: https://www.securityweek.com/medical-practice-closing-permanently-after-ransomware-attack/

3. Brookside ENT and Hearing Center. Permanent closure following ransomware attack. Battle Creek, MI; 2019. Reported in: Bank Info Security, 11 April 2019. Available from: https://www.bankinfosecurity.com/medical-practice-to-close-in-wake-ransomware-attack-a-12321

4. Republic of South Africa. Protection of Personal Information Act 4 of 2013 (POPIA). Sections 19 and 22. Available from: https://popia.co.za/section-19-security-measures-on-integrity-and-confidentiality-of-personal-information/