PracSavvy

Clinical Systems Support and Training

www.pracsavvy.com.au

Edition 114 - February 2026

Happy February everyone. I write this from the middle of the absolute busiest time of the year for me. Registrars and new doctors starting absolutely everywhere and in ever increasing numbers. So apologies to practices who couldn't get the absolute optimum time for software training for their new starters, and a bit of a thumbs down to the GP colleges who last year rebuffed my suggestion for a classroom style clinical software session for their GPT1's. Accommodating this idea would have certainly taken the pressure off me and my vocal chords this time of year.

While I'm being mildly critical, I'll mention the release of "The Health Revolution -20 Year Preventative Health Strategy" by the THS. Actually it's not the final thing, it's apparently an "Exposure Draft", whatever that actually means. Breezing through this 43 page draft (geddit!), reveals not one single measurable goal or outcome although it does mention *equity* and *inclusivity* about 20 times, so it clearly has some merit…

It's quite possible that I'm being unfair in that these documents aren't supposed to contain anything that has to be measured. But it would have been expensive to produce and as always I will be thinking *Opportunity cost*. i.e. how much did it cost to produce and what could that money been used for instead. It's hard to see it as anything other than yet another motherhood statement, deriving it's inspiration from the old Beach-boys classic Wouldn't it be nice. And yes I know that is a *really* dated cultural reference.

I'm a big believer in "control the stuff you can control", so it was mildly annoying to me to see the latest PHN newsletter talk about the CHAPS team now being referrable via the HL Smartforms ereferral mechanism. Normally this would be all good news, but it had been flagged in the GPLO newsletter back in November in far more instructive terms. (click the link if you want to subscribe to the 2nd most useful newsletter going around!). That isn't the real gripe though, the more information link on the article took you to the THS website where, under Referral, you were told to download a pdf form to complete!!. This is exactly the sort of thing that confuses and irritates GP and wins this weeks "shoot yourself in the foot" award.

Speaking of the southern GPLO newsletter the January issue advised the following ereferral changes:

- Addition of Zoledronic Acid Infusion under Ambulatory Care Centre Services
- Addition of Tasmanian Community Paediatric Service/ Kids Care Clinic under Paediatric Services.
- **Back Pain Assessment Clinic** (BAC) - Direct referrals from GPs are not currently possible. Please send the referral to Rheumatology or Neurosurgery and it will be internally re-directed to BAC for triage.

The newsletter also highlighted that Community Paramedic *Post Encounter Discharge Summaries* are now to be sent to General Practice via Healthlink. Whilst a welcome improvement in communications, the fact that these aren't automatically sent to MyHR as well, means there is no cherry on an otherwise reasonably delicious cake.

Speaking of MyHR, the Digital Health Agency have released a couple of new free online courses around MyHR, a) In the Age Care sector specifically and b) as a general reminder of MyHR and rules and regulations around it. The second course is not the worst half hour revision exercise on the whole thing and may well freshen up staff knowledge on this topic.

Speaking about things that are at least MyHR adjacent, this month saw the flagging of a National Medicines Record ostensibly off the back of a tragic suicide using stockpiled drugs story from last year. I do wonder what this record could contain that isn't already in the MyHR. There is some thought that online health providers aren't sending prescription information to MyHR. The thing is, if they are generating scripts, these go through the ERX system which is a data feed to MyHR. A further opportunity for MyHR upload also exists at the dispensing stage from the pharmacy software. Unless the telehealth operator has specifically flagged the script as "not for upload" I don't know how this would happen

What certainly may be the case is that the online prescriber is not up-loading the "Reason for Prescription" to MyHR. Telehealth doctors wouldn't be the only ones not doing this though and we also have to mention that about 9% of the population doesn't have a MyHR. *continued*

Continued..

I really hope that they have the right people in the room when they strategise all this and don't spawn mass confusion by creating another big system sitting alongside MyHR. There are certainly things that GPs can do to mitigate medicine errors (see below) and it's worth noting now that apparently 7% of Australians are meeting the definition of polypharmacy (one of the definitions at least). My wish list for system improvements might look like this:

a) Combination of all the safescript (TasScript et al) databases into a truly national system.

b) A dynamic MyHR report that runs interaction checking on all current medicines and illnesses recorded in the MyHR.

c) A prompt in the GP software that the MyHR level Interaction report has identified something (possibly colour-coded for seriousness)

d) Increased promotion and education to Health Professionals around the Active Script List (ASL)

e) All patients on schedule 8 drugs have to have a MyHR with medicines information not hidden. (Wouldn't get past the privacy freaks, but a man can dream can't he!)

In more news there was an interesting report on the number of fully bulk-billing practices in Australia, and more importantly Tasmania. According to the 2026 Cleanbill report Tasmanian fully bulk-billing practices rose from zero to 33% as a result of last years BB initiatives. Quite a transformation, undoubtedly in part at least off the back of decisions taken by one of the bigger corporate groups.

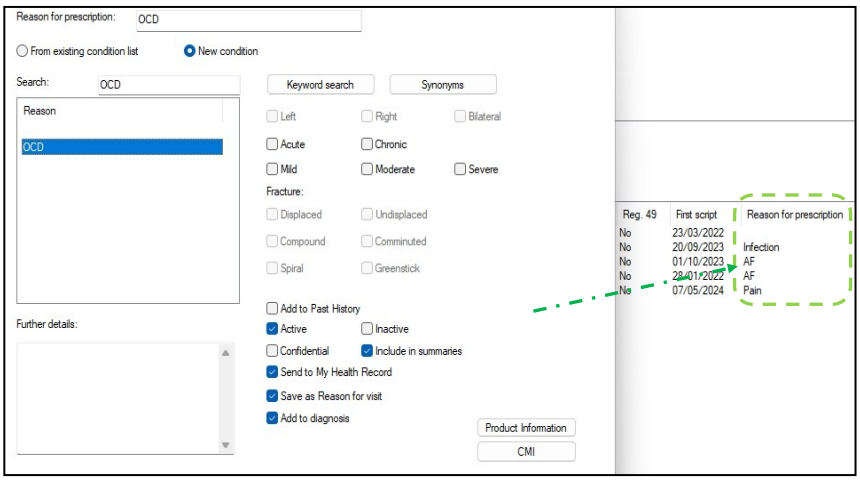
Lastly this month, page 4 is a sobering article around the nature of technology threats that exist for businesses in 2026. Thanks to Mathew Russell for sharing this from the prevention front lines.

BP

Before we get started on the medication management theme, I just wanted to repeat the **important reminder** that practices should ensure they have run the PRODA TLS Security Update Utility by February 3rd if they want their Medicare connectivity to keep working.

It seems pertinent to remind GPs of some of the steps that can be undertaken to optimally share recorded medication information (especially prescribing context).

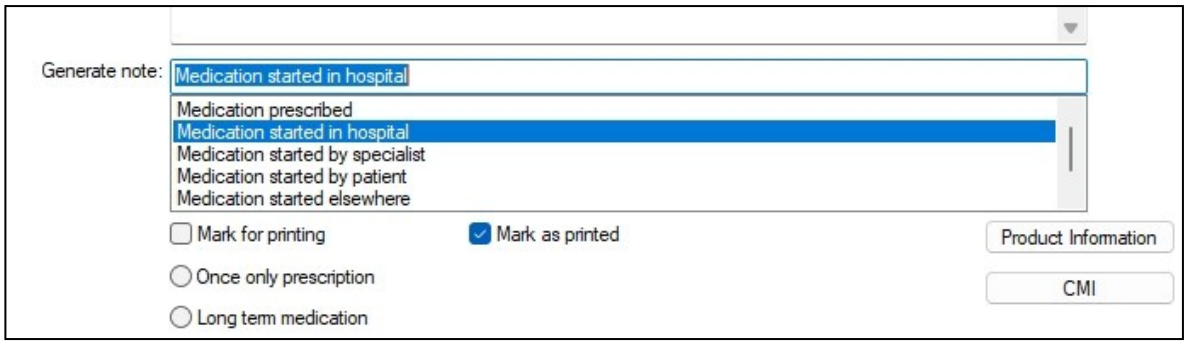
1) Reason for Prescription - It troubles me that some GPs don't complete this final screen in the prescribing wizard. Even if the relevant condition is already reflected in the *History*, completing this step places the *clinical context* at the end of the medication information line. This context will also find it's way to the MyHR via the prescription record (from ERX) and also via any uploaded *Shared Health Summary*.



Don't forget to decide whether the condition also needs to be mentioned in the Past Medical History. You can also use this for entering *Your Reason for Visit*. If you can see that some medications are showing no prescribing context, you can right-click the medication in the list and select the *Edit Reason for Prescription* item. This could even form the basis of a small QI activity.

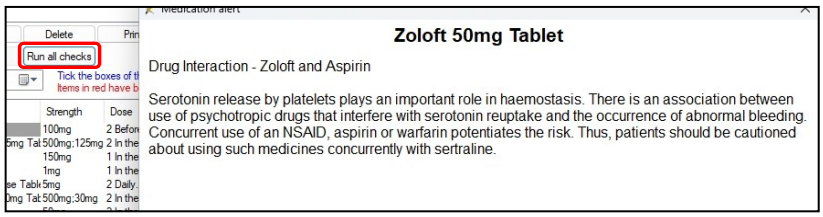
Continued..

2) Prescribed elsewhere - Remember that the patient's record should reflect all medications that they are taking, not just the ones prescribed by you. This means that the automatic interaction checks run by BP will reference all the medications the patient is taking. To add a medication to the patient's current list just change the settings in the prescription wizard as shown below.



This will result in an addition to the medication list without the generation of a script. This information will also be shared with others if a Shared Health Summary is uploaded for the patient. Older Doctors should be in no doubt whatsoever about the utilisation of MyHR information by emergency room doctors.

3) Run all Checks - A really good feature of BP that is sometimes neglected is the Run all Checks button which re-runs all the standard interaction checks that are done between the Medication and History lists.

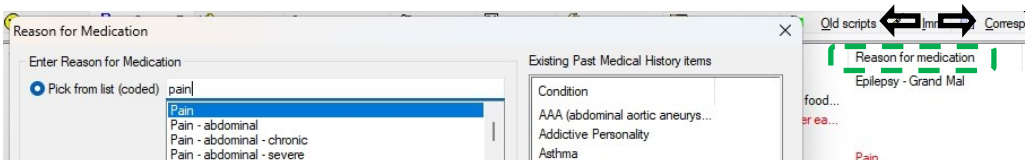


Additionally there is more checking if you are running the Primary Sense tool and haven't opted out of medication prompts.

MD

Here are the relevant screenshots for MD users.

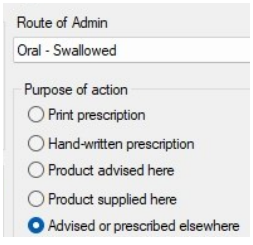
1) Reason For Prescription



Happily MD mandates that you provide a Reason for Prescription. Note that you may find the Reason for Medication at the far right of your MD display. One of the nicer features of MD is that you can drag these column headings into a position on your screen that you prefer and MD will remember your preference. I would certainly move this field so that it was in my immediate field of vision.

2) Prescribed Elsewhere.

Running out of room, but easy to see.



Mathew Russell runs an IT support company based in Queensland providing tech support to dozens of practices. He recently sent out some updated security advice and reminders to his clients. I'm sharing it here with his permission.

Considering the ongoing evolution of cyber threats, particularly those targeting the healthcare sector, I wanted to share a timely reminder and key observations to help safeguard your practice, staff, and patients.

Recent reports (including Microsoft's 2025 Digital Defence Report and Sophos' State of Ransomware in Healthcare 2025) highlight a sharp increase in sophisticated attacks, with **over half of known cyberattacks** driven by extortion and ransomware. Healthcare remains a prime target due to the critical nature of operations and the high value of protected health information (PHI).

Key Developments in Current Threats:

- Attackers have advanced beyond traditional ransomware (encryption-only). They now frequently employ **double-extortion** tactics: stealing sensitive data before encrypting systems and threatening public release if ransom demands are unmet. This has proven particularly damaging in healthcare, where exposure of patient records can lead to severe reputational, regulatory, and legal consequences.
- A growing trend in 2025 is **extortion-only** attacks (no encryption), which tripled in healthcare incidents compared to prior years, capitalizing on the sensitivity of medical data without the complexity of full network disruption.
- The primary entry point remains **highly convincing phishing emails**, often mimicking legitimate communications. These frequently include:
  - Attachments or links claiming to contain encrypted documents (e.g., PDFs or scans).
  - Redirects to fake Microsoft 365 or Google Workspace login pages requesting full credentials to "decrypt" or "view" content.
- **Critical red flag:** Legitimate Microsoft 365 or Gmail decryption/verification processes **never** require entering full usernames and passwords. They use only email address entry followed by a one-time verification code sent via email or app.

Recommended Best Practices to Mitigate Risks:

- **Phishing Awareness:** Train all staff to immediately close and delete any email requesting full login credentials for decryption or access. Verify suspicious requests directly with the sender via phone or known contact.
- **Email Hygiene:** Avoid storing sensitive patient communications in inboxes or sent items. Immediately delete emails once patient data has been imported into your practice management system (e.g., BP or MD). Email accounts remain a common initial compromise vector, even with strong perimeter defences.
- **Data Storage Security:** Ensure no unencrypted patient information resides on local PCs, servers, or network drives outside of secure practice management software. Immediately delete incoming documents, faxes, imports, or exports after processing.
- **Overall Vigilance:** Adopt a "zero-trust" mindset—second-guess every unsolicited email, link, or attachment. Regular staff training and simulated phishing exercises are among the most effective defences.

Insurance Considerations: While cyber insurance typically provides coverage for breaches, policies often include exclusions or reductions if the incident stems from negligence, such as storing sensitive data insecurely or failing to follow minimum security standards. Demonstrating robust data-handling procedures strengthens both your defences and your claim position.

Thank you for your continued partnership in protecting patient privacy and practice integrity