Optometry AUSTRALIA

Secure information exchange: What you need to know

The following information provides an overview of your legal obligations regarding the secure electronic exchange of information and preliminary advice for sending and receiving information electronically, such as referrals.

To assist optometrists adopt best practice information exchange moving forward, Optometry Australia is currently collaborating with practice management software vendors and messaging service providers to:

- *Facilitate links between practice management software vendors and messaging service providers to support the implementation of secure messaging into optometric practice management systems;*
- *Advise practice management software vendors and messaging providers about the practice and clinical needs of optometrists regarding communication processes and the exchange of patient information; and*
- *Investigate opportunities to establish formal arrangements with preferred messaging service provider(s) to benefit OA members.*

We encourage you to contact your practice management software vendor to let them know that secure messaging is important to help you meet your privacy obligations, support efficient practice communication processes and the effective management of your patients.

Electronic exchange of personal information; what are my obligations under national law?

There are various privacy laws that regulate the collection, use, disclosure and storage of personal information by individuals, and private and public organisations, including optometry practices; most notably the *Privacy Act 1988*, Australian Privacy Principles (APPs) and the *Electronic Transactions Act 1999*. The provisions set out in these laws also apply to the electronic exchange of patient information between health care providers and from a health care provider to a patient.

Principally, health care providers and entities must take ‘reasonable steps’ to protect patient information from unauthorised access, modification or disclosure. This includes information sent or received electronically such as a patient referral.[1] With regard to electronic information exchange, ‘reasonable steps’ may include:

- Secure messaging technology
- Email security measures (e.g. encryption, email disclaimer)
- Patient de-identification measures
- A practice policy on secure information exchange
- Staff training and education on information security
- Record keeping regarding external email traffic flow

[1] Australian Privacy Principles. No. 11.

The Office of the Australian Information Commissioner (OAIC) has developed a resource titled ‘Guide to securing personal information’ to assist individuals and organisations to better understand their privacy obligations under national law. The OAIC states that standard email is not a secure form of communication and that entities should have policies and procedures in place that govern the secure exchange of information via email.

What should I be doing now to ensure I meet my privacy obligations when sending or receiving information electronically?

Optometry Australia recommends all electronic transmission of sensitive information, such as sending a patient referral, is secured using a form of encryption, preferably through a virtual private network via secure messaging. Secure messaging refers to the ‘point-to-point’ transfer of clinical information from one health care provider or organisation to another over a secure network. The information being sent or received is directly integrated into the practice management system. We recommend you contact your practice management software vendor to discuss secure messaging options.

Optometry Australia does not recommend the transmission of patient information by unsecure email. Sending patient information by unsecure email should be considered a last resort, such as in emergency situations and efforts should be made to validate the email address with the recipient before sending. The RACGP also does not recommend the sending of unsecure clinical information via email.[2,3] Optometrists should be wary that sending unsecure information via email is not only is problematic for the sender, but can also be an issue for the receiving healthcare provider or practice, given the scope of obligations under privacy law. There have been reports of GPs lodging complaints when other healthcare providers have sent them unsecured clinical information such as patient referrals by email.

If your practice management software is not yet integrated with secure messaging technology then you may wish to consider email encryption as an interim measure only. Given the lack of industry standards and the significant variation in email encryption software, there are likely to be a number of security pitfalls associated with email encryption and therefore Optometry Australia does not recommend email encryption as a permanent solution for secure information exchange.

What is secure messaging and what can it be used for?

Secure messaging is the ‘point-to-point’ transfer of clinical information from one health care provider or organisation to another over a secure network. Using a secure messaging system allows healthcare providers to securely exchange clinical information directly to and from the practice management system. It is an important mechanism that underpins a number of ehealth functions and is a being increasingly adopted by healthcare providers as the standard practice for sharing clinical information securely and efficiently, steadily replacing paper-based information sharing. Depending upon the practice management software, secure messaging can be used to securely send or receive clinical documents such as an electronic referral (known as an eReferral), test results and patient summaries.

Secure messaging provides a superior level of protection and reliability compared to an encrypted email, as it provides secure point-to-point information exchange directly into the practice management system. Secure messaging uses a virtual private network (VPN) to send and receive information, significantly reducing the risk of unauthorised interception and also provides the sender with an automated notification when the information has been received by the intended recipient successfully.

[2] RACGP. Practice Standards 4th edition. Information security.
[3] RACGP. Computer and information security standards, standard 6.

What are the benefits of secure messaging for my practice?

There are multiple benefits of using secure messaging for your practice communications including:

- Improving the security and privacy of your patients' clinical information;
- Ensuring you comply with relevant privacy law and regulations;
- Improves workflow efficiency by reducing the burden of paper-based communications and the need to 'chase' referrals;
- Automated notification of successful message delivery; and
- Improving communication, collaboration and trust with other healthcare providers.

Is secure messaging interoperable with optometry practice management systems?

Optometry Australia is collaborating with practice management vendors to encourage and support where possible the integration of secure messaging into optometric practice management systems. We encourage you to also contact your practice management software vendor to let them know that secure messaging is important to help you meet your privacy obligations, support efficient practice communication processes and the effective management of your patients.

The two most commonly used practice management systems in private optometric practice, Optomate and Sunix, may support a certain level of secure messaging interoperability depending upon the version of practice software. Neither system is currently integrated with a single messaging service provider - although this may change in the future so consult your practice management software vendor for the latest update.

As practice management systems overtime become more interoperable with the national ehealth system and messaging service providers, it is envisaged that optometric imaging such as retinal photography and OCT scans will be able to be securely sent via secure messaging and directly imported into the receiver's electronic patient record.

How can I adopt secure messaging for my practice now?

As mentioned, Optometry Australia is currently working with practice management software vendors and messaging service providers to help progress the implementation of secure messaging functionality into optometric practice management systems. Our long-term vision is for all optometric practice information systems to be integrated with secure messaging technology allowing the easy and effective exchange of information.

In addition to our current efforts to link practice management software vendors with secure messaging, a private optometric practice may be able to integrate a preferred secure messaging provider into their practice management software on their own accord. For those considering this option we recommend you:

i) Be clear about your requirements for secure messaging;

ii) Consult your practice management software vendor to find out:
   - Whether your practice software currently supports secure messaging;
   - If your vendor has any plans to integrate their software with a preferred messaging provider; and
   - If any additional technical requirements for your practice management system are needed and what the associated costs are.

iii) As there are number of different products in the secure messaging market, do your own research and investigate the pros and cons of different messaging service providers, including cost. Ensure the product your needs and is compliant with all privacy obligations and national standards. Make sure you also understand the compatibility limitations of each messaging service provider with regard to both sending and receiving information.

iv) Consult your local Primary Health Network regarding the most common secure messaging technology used by your local health care community (e.g. GPs); and

v) For more general information about secure messaging technology in health care, contact the National E-Health Transition Authority (NEHTA).

How much does secure messaging cost?

The cost of secure messaging will vary depending upon the messaging service provider and your practice needs. Costs may include a set-up fee, an annual fee, an item cost per message sent and an item cost per message received. As a general estimate, the total average cost may be a few hundred dollars per annum. Optometry Australia is currently investigating opportunities to establish formal arrangements with messaging service provider(s) that benefit OA members.

Is there an industry standard for secure messaging?

Yes. The National E-Health Transition Authority (NEHTA) in collaboration with Standards Australia has developed a set of industry specifications for secure messaging capability known as 'Secure Message Delivery' (SMD).[4] SMD aims to ensure healthcare providers can communicate and share clinical information securely and efficiently, independent of the type of messaging service provider adopted. SMD is also compatible with the national ehealth record system and ensures messaging service providers comply with all relevant privacy and ehealth legislation (e.g. *PCEHR Act 2012*). Check the eHealth Product Register (SMD) for a list of messaging service providers who are compliant with SMD.

Despite the establishment of SMD, some compatibility conflicts are still present, mainly due to unresolved commercial differences between different providers. It is expected these differences will be resolved overtime and that SMD will become the norm. The important thing is that you understand any current compatibility limitations amongst different messaging service providers.

For information, contact Optometry Australia or your practice management software vendor.

[4] Standards Australia. AS 5552-2013 E-health secure message delivery.