Irish College of GPs

Coláiste Dhochtúiri Teaghlaigh Éireann

Use of Email in General Practice

National GPiT Group

Use of email in general practice

Email is an important, useful and convenient method of business and personal communication for transfer of messages and documents. However, in a general practice setting, there are specific issues to consider including confidentiality and security, professional boundaries, and duty of care.

GPs may receive emails from patients, other clinicians and other relevant third parties which either contain or request medical information. The use of email in general practice has significantly increased in recent years, therefore it is important to consider how GPs can reduce any risks associated with this.

Risks associated with email

- It can be easy to send an email to the wrong email address (and therefore to the wrong person). This may be considered a data breach.
- Emails may be stored, printed or forwarded to unintended recipients. An email may be edited during this process.
- Email content may be visible on stolen or unattended devices such as laptops, tablets or mobile phones.
- There is risk of inappropriate access or interception of email when using widely available email services.
- Email is vulnerable to attack by cybercriminals to spread malware and to scam the unprepared. 90% of malware attacks are launched by email.

Healthmail

Healthmail is a secure clinical email service that allows health care providers to send and receive patient identifiable clinical information in a secure manner. Healthmail messages are encrypted as they travel across the internet within a closed private network and are stored securely at rest.
With a Healthmail account, messages can only be sent to and received from other Healthmail accounts or from hospitals and agencies (e.g. pharmacies, nursing homes and other community health care professionals) which are securely connected to Healthmail. That list is available here:
https://www.ehealthireland.ie/technology-and-transformation-functions/access-to-information-a2i/healthmail1/
However, note that it is possible for emails to be forwarded on by recipients who do not have an @healthmail.ie email address.

Since the introduction of paperless transfer of prescriptions to pharmacies, nearly all GPs will have a Healthmail address. If not, GPs can register for an account at https://www.healthmail.ie/

It is important that practices implement good Healthmail practices. When a GP registers for a Healthmail account initially, they will most likely have a GP named and practice named

address. These addresses form part of a directory from which other health care professionals may try to contact a GP, therefore

- GPs should ensure that all Healthmail accounts are checked regularly
  or
- Use auto-forwarding to an account that will be checked regularly (e.g. from an individual GP Healthmail to practice Healthmail account)

IT Protections

IT measures that may be used to increase security and reduce risk when using email accounts other than Healthmail include

- A spam filter – built into many proprietary email clients.
- Internet security suite which includes anti-virus software. We would recommend a paid internet security suite be used in practices for better protection.
- Encryption and Password Protection of messages, using an encrypted email service or encryption software.

Your IT provider can advise on suitable products.

Practice Policy

Risk can be reduced by applying a practice email policy, either stand-alone or as part of a wider policy on use of the internet and electronic communications. The principle of such policy is to understand and assess the risks associated with the use of email both generally and individually.
Not all email communication carries the same risk, but consideration should be given to:

- Communication of patient identifiable healthcare information via unsecured and unencrypted email should be avoided.
- Other methods of communication (e.g. phone, video or face-to-face) should be encouraged for clinical queries
- If email is to be used, obtain patient consent to any communication by email, and password protect any email that may contain personal information
- Verification of patient email addresses before sending email
- Transcription of relevant emails, particularly if clinical, to the patient healthcare record
- Any email communication should not breach the principles of the EU General Data Protection Regulation (GDPR) and the Irish Data Protection Act 2018
- There is higher risk with use of a device not connected to the practice network for email received that is not from a known or trusted source, and for personal email.

The use of email is part of running any business in the 21st century. It is up to individual practices as to how it is adopted securely. Appropriate time should be given to the management of email, however if used well this may also be a time-saver.

References:

Irish College of GPs *Processing of Patient Personal Data: A Guideline for General Practitioners:* https://www.irishcollegeofgps.ie/Home/Explore-the-College/General-Practice-Management/IT-E-Health/Data-Protection-and-GDPR

Medical Council *Guide to Professional Conduct and Ethics for Registered Medical Practitioners* https://www.medicalcouncil.ie/news-and-publications/publications/

RACGP *Using email in general practice* https://www.racgp.org.au/running-a-practice/technology/business-technology/using-email-in-general-practice

Medisec *Communications via email* https://medisec.ie/gp-resources/communications-via-email-3/