This matrix is to assist practices in determining the level of privacy and security required in order to use email in general practice for communication. The matrix is intended for use as a guide of a general nature only to flag issues for GPs and general practices for further consideration when using email.

Will your practice use email with patients, other healthcare providers and external organisations?	Email Policies and Processes	Additional Guidance	Privacy and Security risk to Practice
No email communication will be used & is not intended to be used	*Not required*	*Not required*	*None*
Email communications with patients is undertaken	No formal policy, no supporting resources, communications undertaken **without the use of passwords or encryption.** Inadequate steps taken to ensure email addressof recipient is correct or email is sent to a generic inbox.	No password or encryption creates a risk that if the email is intercepted in transit, it can be easily be read Emails may be sent to the wrong person or could be read by an unintended recipient.	**High**
	Documented policies and resources exist, **no written consent is obtained or recorded**, email communications undertaken without the use of passwords or encryption.	No password or encryption creates a risk that if the email is intercepted in transit, it can be easily be read by unauthorised person.	**Medium - High**
	Documented policies and resources exist, **consent obtained and recorded**, email communications undertaken **without** the use of passwords or encryption. Email address is verified by the practice.	Pre-written information document available. For example "discussed the privacy risks of the use of unencrypted email, patient is aware of same and requests the use of unencrypted email for communication" Consent documented in Electronic HealthRecord.	**Low-Medium**
	Documented policies and resources exist, **consent obtained and recorded**, email communications using a verified email address is undertaken **with** password protection.	Password provided by another channel i.e. In person, phone or SMS Secure method	**Low**
	Documented policies and resources exist, email communications undertaking using desktop software encryption or via a secure website [TLS(https)]	Very secure method	**Very Low**
Email communications with other healthcare providers and third parties is undertaken	No formal policy, no supporting resources, communications undertaken **without the use of passwords or encryption**; Inadequate steps taken to ensure email address of recipient is correct or email is sent to a generic inbox.	No password or encryption creates a risk that if the email is intercepted in transit, it can be easily be read. Emails may be sent to the wrong person or could be read by an unintended recipient.	**High**
	Documented policies and resources exist, **no consent obtained**, email communications undertaken without the use of passwords or encryption	As above	**Medium-High**
	Documented protocols and resources exist. Secure messaging software with digital credentials is used.(Refer to RACGP Guide to Secure Communications – Product List)	Very secure method	**Very Low**
Communicating using Government Databases			
Medicare Online, HPOS	Medicare Digital Credentials (PKI)	Highly secure method	**Very low**
Personally Controlled Electronic Health Record (PCEHR)	NASH (PKI)	Highly secure method	**Very low**