GDPR, email and private practice

A new set of data protection regulations became law in the EU (including the UK) in May 2018. General Data Protection Regulation (GDPR) replaces the 1988 Data Protection Act. The regulation brings new rights and expectations about how our personal data is collected, transmitted, stored and deleted.

The Information Governance leads of NHS Trusts have been busy over the last few months, ensuring processes and policies have been updated. It is likely we will see changes in our mandatory training programmes over time.

One of our readers recently asked if I could advise on how he could continue to send emails containing private patient information between himself, secretaries and private hospitals. The question was in respect of the new GDPR legislation. This issues Tech Review attempts to provide some guidance on this scenario.

Interpretation of GDPR

The regulation stops short of specifying exactly what security technologies are considered acceptable in different situations. This is by design, as technology is constantly changing. Specific requirements will become clear once GDPR is used in UK legal cases, creating new reference case law. The services I describe below are those I would use in the email scenario laid out above. The practices described are those of this author and not necessarily the views or recommendations of *Eye News* or the publisher Pinpoint Scotland.

Key GDPR principles

Data protection by design

The GDPR states that there is an obligation to implement technical measures that integrate data protection into the processing of data. Even though the regulation does not specify the precise requirements, when considering email, end to end encryption would be a reasonable expectation. Standard email or the use of fax would almost certainly be considered insufficient.

European servers

The GDPR regulation is easier to comply with if all personal data reside on servers based in the EU. There are situations where services based in other countries are allowed, but these are the exception and not the rule.

Right to erasure

The GDPR provides the right for individuals to have their personal data removed from a service. This right does not apply in all circumstances, and healthcare is one such area. Healthcare providers have a duty to store medical records for a number of years (depending on age and type of record). This requirement is felt to override the right to erasure, and is therefore not something our surgeon working in the private sector needs to be unduly concerned about.

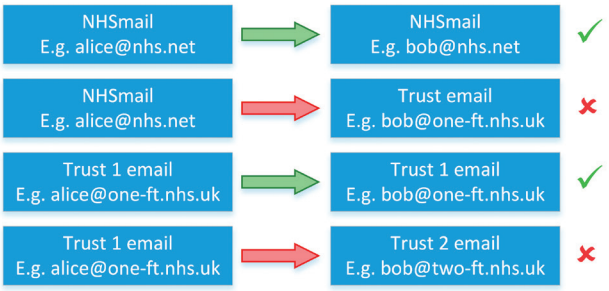

Figure 1: Which email routes are secure? Green secure, red not secure.

Use of existing tools

In NHS practice, personal data can be securely sent in email from one NHSmail address to another. Equally, the same degree of security is typically present when sending email from trust email to trust email. This is only the case when the trust is the same. Figure 1 illustrates this point more clearly.

In private practice, all parties are unlikely to have NHSmail or a single trust email account. Some businesses buy encrypted email services. An example of such a service is Egress Switch (by Egress.com). If a private institution uses Egress and provides their doctors with paid accounts, this would be a good solution. The doctor could communicate with anyone via secure email, as long as the doctor's account was a paid Egress Switch account. Recipients without paid Switch accounts could still reply (with security) as long as the original sender retains a paid Switch account.

Using email to share personal data without a provided solution

In the absence of a suitable provided solution, it is quite straightforward to set up your own. Although the Egress Switch service is primarily a corporate solution, it can be used for £80/year for a single user. Arguably a better, and lower cost, option is to use ProtonMail (PM). This secure email service is free for a basic use and €48 per year (or €5 per month) for more advanced use. The basic features will be enough for most and would allow a user to get started. ProtonMail state that all user data is stored exclusively on European servers. PM is the service I would use in this scenario.

What about imaging?

Emails are used for sending more than just personal data in the form of text. We use them to send imaging data, such as OCT reports and photos. The same rules apply to this type of data. In addition, there are questions around the attachment file size limits. Many of our ophthalmic PACS products allow exporting of files which can then be attached to emails. If the choice is available, it is often best to choose a .JPG file, rather than a .TIF file. The former results in a much smaller file, with a small degree of quality reduction. Although .TIF files are slightly higher quality, the file size it typically so large that sending them over email becomes very difficult.

Protonmail has a 25MB attachment limit per email. NHSmail has a 35MB per email attachment limit.

GOT A TECH QUESTION?

If you have any topics or questions you feel would be appropriate for the tech column, do get in touch.

SECTION EDITOR

David Haider,
Consultant Ophthalmologist and Chief Clinical Information Officer, Bolton Foundation Trust, UK.
E: david@drhaider.co.uk
Twitter: @drdavidhaider

The author has no proprietary or financial interests in the products discussed.