May 2012
Approved

Frequently Asked Questions on new guidance for email in NHSScotland

1) Why the need for new guidance?

There is confusion as to what can be sent between NHSScotland boards, to business partners and patients. Taking the line "that it is only permissible to send patient information to a user with the same email service" is not practical given the breadth of partners the NHS has (and has never been NHSScotland 'policy'). Far from withering away as some pundits have predicted, email is still growing in importance in healthcare as a means to transact essential business. We need to use email more as part of our eHealth strategy while being mindful of the real rather than imagined risks. NHSScotland needs to take the lessons learned from actual privacy and security risks relating to email (e.g. recent Information Commissioner's Office enforcement).

2) Does the guidance differ from anything 'official' that currently exists?

There has never been an official NHSScotland-wide policy and each board has its own policy. The aim of this guidance is to fill the void with a national approach based on good practice which can be tailored locally.

Some boards, mainly those on NHSmail, have in the past taken a steer from the former Connecting for Health (England), as to what is and what is not permissible. But this guidance supersedes any legacy documentation and is specific to the needs of NHSScotland. Vendors and agencies such as National Services Scotland (which is in effect an internal supplier for an email service used by some but not all boards) follow the policies and guidance agreed by governance structures of NHSScotland.

3) Will the guidance become obsolete given a new email service for NHSScotland is planned?

No, the guidance stands regardless of what type of email service will be used in NHSScotland once the nhsmail service (used by some but not all boards) ends in 2013/14. Even if all NHSScotland boards signed up to a single service provider in the future there will always be business partners and patients with various email addresses who need to be contacted. This guidance places great weight on the handling instructions and not simply on which email service is used.

4) What is the biggest security/privacy risk relating to email in NHSScotland at the moment?

Without a doubt the biggest risk is sending patient identifiable information to the wrong person through human error, lack of employee training and poor business processes. The recent Civil Monetary Penalties issued by the ICO bear this out. This can be a manual error, such as simply clicking on the wrong copy list, not checking with a manager whether such data should be sent in the first place (e.g. bulk data in

a spread-sheet) and including far more data than was strictly necessary for the purpose (e.g. enclosing detailed case notes on a patient when a simple confirmation about someone's appointment/status of treatment would have sufficed).

5) So how does the guidance address these risks?

The guidance places great emphasis on handling instructions via three steps. The first to understand the relative sensitivity of the information, the second to be clear about who you are sending it to and in what quantity (e.g. one patient = one email, checking who are trusted as opposed to un-connected parties) and thirdly checking the email suffix as the level of technical security is still relevant.

6) Does the guidance permit emailing patients for the first time?

There has never been a NHSScotland policy preventing use of emails for patient contact. Instead, there has been a recognition that boards do not currently have the infrastructure for high volume email services but that it is something to be developed incrementally. This guidance provides some simple ground rules and recognises the value that email for patients can bring to eHealth at the lower end of sensitivity. It also makes clear the areas where email is still not appropriate given security and confidentiality concerns.

It also needs to be stressed that none of the alternative channels such as paper letters sent by normal post are necessarily any more secure (e.g. high volumes of letters lost or sent to wrong persons). Instead, sensible risk based decisions need to be made on the right communication channel for the purpose.

7) How do issues of patient consent operate in regard to email?

There is no change here. The NHSScotland Code on Patient Confidentiality (updated 2012) makes it clear that consent can be both implicit and explicit, written and un-written.[1] The guidance recommends that patients give consent where email is to be used as it is still a relatively ad-hoc tool for specific purposes at the moment. But consent can be obtained in many ways and does not need to be bureaucratic (e.g. ongoing dialogue between clinician and patient). The most important thing is that patients understand how and why a communications channel is being used and their preferences are respected. Indeed, in the case of some patients with disabilities such as impaired or loss of sight email can be both more secure and accessible than traditional paper (i.e. because the user may have software to enable it to be read rather than having paper sent to a shared building and read out by another person).

8) Can I use my own personal email account?

No, the guidance and accompanying tables make clear that all work-related email communications must be through your official NHSScotland email account (which can be either nhs.uk or nhs.net).

---

1 http://www.knowledge.scot.nhs.uk/media/CLT/ResourceUploads/4011563/Revised%20Code%20of%20Confidentiality%20-%20Final.pdf

9) Does the guidance simply list which organisations I can email to?

No, instead it discusses the need for boards to determine who are trusted partners and the importance of having information sharing protocols. All NHScotland boards are considered as trusted partners by default (whether they use nhs.net or nhs.uk official email accounts). For other partners an information sharing protocol (e.g. with a local authority, constabulary or charity) would among other things agree on the types of information to be shared, the sensitivity and look into the mechanics of emailing (e.g. designated email accounts, file formats etc.).

10) Is it true that email is only 'secure' where encryption is used?

This is not strictly true. We need to get away from the simplistic notion that the 'presence of encryption = good security' and the 'absence of encryption = poor security'. There are lots of factors which make email more or less secure. Following the handling instructions is most important. No amount of encryption of data while it is on the move for example will help if the email is simply sent to someone who is not entitled to see it by mistake. The accompanying tables take a risk-based approach based on what is known about the infrastructure that is used when an email is sent. For example, we know that where an email is sent from a health board in Scotland to many business partners that public-sector (i.e. health, local government etc) networks are invariably being used or are covered by an equivalent standard (e.g. GSx) so the absence of encryption in each and every case poses a low and manageable risk. Many of the these networks, such as N3 and the government GSi work on codes of connection and other factors to minimise risks rather than deploying encryption.

The tables have been designed so that the user just needs to check the email suffix and look for the tick or the cross (rather than second-guess things such as encryption which is a complex matter).

11) If encryption is not always present then why is it relevant at all?

There are two types of encryption which are relevant here. Firstly, encryption of information 'on the move' (i.e. while the email is carried across the wires or in the air) scrambles and then re-assembles information so that it cannot be read if it is 'captured' without a key. In order to capture an email *en route* a person needs to be skilled and motivated enough to want to do this. There is no evidence to date of anyone acquiring NHSScotland information via this method but we know it is possible under certain conditions. In order to mitigate the risk of this happening we can use in-built transport encryption (if all parties use the same email service) or get both senders and receivers of email to both agree to downloading software such as S/MIME 'certificates'. The difficulty here is that not all of our partners such as third sector and patients will ever use the same email service so sensible risk based decisions need to made if we want to continue providing a range of health services.

The second type of encryption relates to 'locking' information up prior to sending in a file for example. This ad-hoc method does have its place (which board Information Security Officers can advise on) but is not without its problems. For example often such files are filtered out by email service providers and do not have proper handling instructions (e.g. sending the 'key' to open the file via an email rather misses the point of sending a locked file in an email!).

12) Does the absence of encryption mean that people can 'hack' into my emails?

There has been much media discussion about 'hacking' into emails by agents working for newspapers. In virtually all cases this has been a matter of gaining a person's login details such as username/password or other credentials or with help from an insider (e.g. system administrator or someone who manages an email service) rather than actually eavesdropping or intercepting an email while it is on the move. NHSScotland has separate guidance on minimising the risks through better authentication controls and the risks of social media.

13) Does this guidance now mean that NHSScotland boards need to start using government protective markings for every email?

No, the guidance recognises that *some* of our business partners such as local government and the police do use the Government Protective Marking Scheme. The NHS needs to be able to align its information to that scheme to enable information sharing. We know from experience that poor alignment (e.g. inappropriate use of the word 'Confidential' or considering everything Restricted) undermines information sharing. Similarly, using the 'sensitivity' labels used by email clients such as Microsoft Outlook (i.e. 'normal', 'personal', 'private' etc) are meaningless and should not be used.

The simple traffic light approach (understanding what is 'Red', 'amber' and green') helps the staff who makes judgements on relative sensitivity.

For all normal intra-NHSScotland business protective labelling may not be deemed necessary. Although, a better understanding of what is 'red' and 'amber' does focus the mind on relative sensitivity (i.e. ranging from the routine emails about appointments to the highly sensitive that could significant distress or harm).

14) Are there any cost implications to following this guidance?

No, the guidance is designed to help boards who are updating their local policies rather than asking for new tools to be implemented. Although some additional training and updated materials would be very beneficial (especially for those staff who regularly send patient information to partners outside the board). It is possible that following the guidance could actually reduce some costs associated with sending paper correspondence via normal or tracked mail as more email transactions to colleagues in other boards and to patients become possible at the lower end of sensitivity.

15) What do I need to do now with this guidance?

Share it with all those involved in creating board policies and delivering training materials. Share it with those who create information sharing protocols with external partners as email is likely to be a key channel. Share it with anyone who has a business need to contact patients via email.

DMB