## Emailing and Texting with Patients

<table>
<thead>
<tr>
<th>Trust Board Meeting - Part 1</th>
<th>Item: 8.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 September 2013</td>
<td>Enclosure: I</td>
</tr>
</tbody>
</table>

### Purpose of the Report:
This paper explores the use of email and texting in certain forms of communication with patients. This would enable the Trust to enhance its communications with patients, increase patient satisfaction and improve operational efficiency.

### FOR: Information □ Assurance □ Discussion and input □ Decision/approval ☑

### Sponsor (Executive Lead):
Simon Milligan, Director of Finance

### Author:
Janice Sorrell McLeod, Information Governance Manager

### Author Contact Details:
2728

### Risk Implications – Link to Assurance Framework or Corporate Risk Register:

### Link to Relevant Corporate Objective:
- Improving patient satisfaction
- Improving operational efficiency

### Document Previously Considered By:
EMT, EMC, Information Governance Committee

### Recommendation & Action required by the Trust Board:
The Board is asked to adopt Option 2 for unencrypted emailing/texting with patients in these areas:

a) Email / Texting of appointment reminders
b) Correspondence with Complaints / PALS
Emailing/Texting with Patients

Purpose

1. This paper explores the use of email and texting in certain forms of communication with patients. This would enable the Trust to enhance its communications with patients, increase patient satisfaction and improve operational efficiency.

Introduction

2. Use of the internet and mobile technologies, have become increasingly common in modern society. This means that the Trust needs to find a way of meeting the needs and expectations of patients who are used to texting and emailing, but also to remain compliant with information governance regulations.

3. The Trust is under pressure to increase patient satisfaction and to reduce DNA rates and postage costs and this paper explores the options around email and text communication with patients. In particular the paper only considers the following areas:

   a) Email / Texting of appointment reminders
   b) Correspondence with Complaints / PALS

4. The paper covers the legislation, statutory guidance, guidance from the Information Commissioner’s Office as well as current Trust policies. It considers the options available for balancing patient needs and expectations against these requirements and proposes a practical solution.

The basic compliance required

5. The Department of Health (DH) statutory guidance (NHS Confidentiality: Code of Practice) and the Trust’s Email Policy states that no patient identifiable data should pass unencrypted over the internet (e.g email/text). These derive from the Data Protection Act 1998 - “Principle 7 - appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.” Moreover, it is the position of the Information Commissioner that sending information by email is equivalent to putting it on a postcard and sending it through the Royal Mail. Any information about a person’s health is defined as Sensitive Information according to the Data Protection Act (DPA), the processing of which requires legal basis for processing under Schedule 3 of the Act, the foremost of which is explicit patient consent.

6. The risks of emailing/texting unencrypted information are as follows:
   - Any information transferred out of the Trust’s network is NOT SECURE
   - The text/email is open to physical access by hackers or other cyber products that have the ability to intercept emails/texts without authority
   - Personal information could be intercepted by other family members or friends who have access to the email account/phone
   - The Trust cannot be held responsible for the security of personal information coming into and going out of our network in this case
   - There is no guarantee that the information sent has not been changed before receipt
   - The confidential email(s)/text(s) sent could be forwarded to other members of the public
   - Recipient may be unsure of the sender’s ID and may feel the email/text does not originate from Kingston Hospital.
Current Position at Kingston Hospital

7. To balance the competing demands of information security and ease of access, national best practice (as adopted by the National Cancer Information Prescriptions Team) is that direct opt-in consent (explicit) is required. This reasonably complies with section 3 of the DPA. Here the patient enters their email address and signs a form where all the risks of email are explained. This method has also been approved by the ‘Caldicott 2’ report as an acceptable way for emailing with patients and this report has now been approved in full by the Government.

8. The Trust has an **Emailing Patients Procedure** which too relies on direct opt-in consent. At the Trust, Cancer Services, Main Outpatients, Occupational Health and some Paediatrics services in the Trust use this procedure currently. Also, the Wolverton Centre uses opt-in consent to text results to patients.

   The messages to staff around email are currently:

   - Emailing inside KHT to other KHT accounts is SECURE
   - Emailing from KHT to anywhere else and vice versa is NOT SECURE
   - Emailing from @nhs.net to @nhs.net (and the other accredited links) is SECURE and the only authorised way to email patient information between Trusts. N.B. this would continue as the authorised way of transferring lists of patient details, when required, between Trusts and other accredited organisations.
   - Emailing with patients – only if they’ve signed the emailing patients consent form – this is not fully secure, but the patient has signed to accept the risks

Drivers for change

9. Patients now used to receiving text and email appointment reminders from dentists, GPs and other businesses. They want to be able to email the Trust regarding complaints and enquiries and indeed it may be the only practical means of communication open to some of them.

10. The system described at 7 above, whilst being best practice in terms of compliance with Data Protection and DoH statutory guidance, is increasingly cumbersome in light of modern experience with email and text and patients’ expectation about communications via these channels.

11. From the Trust’s perspective, free (unencrypted) emailing/texting with patients could reduce the Did Not Attend (DNA) rates by sending appointment reminders, reduce postage costs as well as increase patient satisfaction.

How other hospitals approach the email issue

12. Other hospitals fall into one of two broad categories:

   - **Allow restricted email with patients** supported by an emailing patients procedure.
   - **Free email with patients** – using disclaimers on emails and website. Although this alerts people to the potential risks it does not provide proof that they are aware of them. This option is not discussed here as more detailed guidance would have to be developed for staff.
The Trust falls into the first category. The Trust’s initial procedure was developed by the Surrey Information Governance Group and has been deployed in Trusts both in Surrey, London and beyond.

Options

13. The following options are raised for consideration:
   Option 1 – Maintain current approach
   Option 2 - Free email restricted to key areas - Appointments, complaints/PALS

Option 1 – Maintain current approach

14. The Trust continues with its current Email Policy allowing communication with patients only where direct opt-in consent has been given.

Risks
a. Patients may find the consent process cumbersome and choose providers who do not require consent.
   b. Difficult to enforce technically
   c. This would restrict the effectiveness of plans to improve DNA rates and reduce postage costs.

Benefits
a. Compliant with Data Protection Act, DoH Statutory Guidance and Caldicott Report 2
b. Mitigation of potential fines from the ICO should an incident occur.
   c. Patients receiving email and text from the Trust Hospital have consented and are aware of the risks to their confidentiality.
   d. Patients receiving text and email from the hospital have more confidence that the communication is genuine.

15. In addition, the process for acknowledging all email complaints/concerns (received by Executive Team and Complaints/ PALS teams) would need to be changed. Any staff member receiving a complaint via email will need to adopt a more formal process for acknowledgement and this would if best done solely through the complaints office. Two options are:

   - Initial generic acknowledgement of receipt of email – having deleted all content of original email. The advice given in this email would be that further email correspondence is only possible if an email consent form is completed. The email consent form would be attached.

   - Email complaints to be treated exactly as letters – ie no immediate email receipt, but a formal acknowledgement within the requisite 3 working days. As such all emails to be immediately forwarded to the complaints team. The acknowledgement paperwork will include the email consent form as well as the usual information.

Option 2 – Allow unencrypted email/text in these following areas - Appointments, Complaints / PALS

16. The Trust would sanction the use of texting and emailing without direct opt-in consent in a few select areas:
   a) Email / Texting of appointment reminders
   b) Correspondence with Complaints / PALS
17. The Trust would need to i) apply a disclaimer (such as that shown in Appendix 1) on all outgoing emails from all staff (this could be done as a signature in Outlook) and ii) ensure that this was prominently displayed on its website.

Risk
a. The Trust would not be wholly compliant with the Data Protection Act, which requires explicit consent.
b. Should an incident occur the Trust would be more likely to incur a fine as we cannot prove that the patient has read the disclaimer and is aware of the risks of email/texts.
c. There would be no authentication that communication is coming from the patient.
d. Counter intuitively, this may lead to frustration from patients, as we are not allowing full email access on all matters, only those relating to complaints and PALS.

Benefits
a. PALS and Complaints could correspond freely with patients/complainants which would have the potential to improve relationships with complainants. Consent will still be sought from patients to investigate and to access their records.
b. Appointment reminders could be sent by text and email improving DNA rates and reducing the postage cost.
c. Clinic letters being sent by email to patients would reduce postage costs.

In adopting this procedure, i) CRS would need to be adapted to hold the information (mobile number and email address) in readily extracted form and ii) the Trust would need to maintain an opt-out list for both text and email and also check texts against the Telephone Preference Service List.

Discussion

18. Under Option 1, the Trust would be compliant with the DPA, DH statutory guidance and national best practice in terms of patient consent to email, however patients may see signing a form as unnecessarily bureaucratic and the Trust runs the risk of being left behind as more people expect to correspond by email.

19. Under Option 2, the Trust would be able to introduce a more effective and rapid communication with patients, but would reduce its explicit compliance with the DPA and DH guidance. The Trust would minimise this exposure by i) restricting the texting/emailing freedom to the two departments mentioned and ii) using disclaimers as widely as possible. This should support an improved level of patient satisfaction and also has the potential to improve the operational efficiency of the Trust.

Recommendation

20. After due consideration, it is proposed that Option 2 is adopted and that the Trust works up the changes needed to internal policies to minimise potential risks.

Simon Milligan
SIRO
Jane Wilson
Caldicott Guardian
Example

Appendix 1 – Disclaimer on Website and external emails

Please note, the following text would appear on the Trust’s website and be added in full (not as a link) to all emails going outside the Trust:

This is to inform you of the risks involved when sending and receiving personal information electronically.

Risks:

- Any information transferred out of the trust’s network is NOT SECURE
- Your personal information could be intercepted by other family members or friends who have access to your email account
- If you are using a work email account, your employer may have access to these emails and they may be stored and backed up on their system
- Your personal information will be open to access by hackers and by cyber products that have the ability to intercept emails without authority
- The trust cannot be held responsible for the security of your personal information coming into and going out of our network in this case
- There is no guarantee that the information sent has not been changed before receipt
- The confidential email(s) sent could be forwarded to other members of the public
- Your personal information will not be encrypted or sent in a locked file format
- You will not be informed of the exact date the information is sent. It is your responsibility to retrieve the information

Trust assurance:

- A review of the information requested will be carried out and the Trust reserves the right to refuse to email information if deemed inappropriate or sensitive
- A copy of any information sent will be retained in the department file (or in your medical records if related to your care) and the origin of the information will be verifiable
- Information will only be sent from an NHS network email – the address will end with @kingstonhospital.nhs.uk or @nhs.net

By corresponding via email you accept and agree to the following statement:

I agree that Kingston Hospital NHS Foundation Trust can send confidential personal information to me via email. I have read and understood the risks associated with this, as detailed above.