OAKLEY HEALTH GROUP	
EMAIL AND SMS MESSAGING POLICY	
REVIEW DATE:	**02.05.18**
REVIEWED BY:	**Dr N Bhatia**
NEXT REVIEW:	**01.04.19**

RELEVANT LEGISLATION

The Privacy and Electronic Communications (EC Directive) Regulations 2003

SMS MESSAGING

Mobile telephone numbers are collected from patients at the time of registration or opportunistically at any time thereafter.

Patients provide their mobile number for two purposes:

- To allow the surgery to *ring* them on their mobile phone
- To allow the surgery to *message* them (SMS)

1) Fair processing information will be provided to patients regarding the processing of their mobile phone number (the collection and subsequent use).

2) Patients who do not wish to be contacted at all using their mobile phone can either not provide that number or ask for it to be removed from their GP record.

3) Patients can, at the time of registration or *anytime thereafter*, request that their mobile phone number is used only for telephone calls and not SMS messages (i.e. they can opt-out from or, after the 25th May, "object" to, SMS messaging).

4) SMS messaging can **only** be used for purposes of direct medical care.

Examples include:

- MJOG-generated appointment reminders
- Invitations for annual reviews or other regular monitoring
- Invitations for vaccinations (including flu clinics)
- Informing patients of an unexpected cancellation of their appointment

5) SMS messaging **must not** be used for any purpose other than direct medical care, such as general surgery information, events or promotions, or Friends And Family Test (anonymous) surveys. This would be classified as direct marketing**.**

6) MJOG, the software that can be used to send SMS messages, keeps no record of the message sent (i.e. *there is no data retention*).

7) If an individual uses their personal NHS Net account to send an SMS message (assuming they have been enabled to) then the message should be deleted from their sent folder as soon as possible. If a record needs to be kept of the sending of such a message then this should be made directly within the GP record.

8) Care should be taken to regularly ensure that patients' mobile phone numbers are up to date. This is particularly important for children whose mobile number on their GP record might still be one of their parent's numbers, when in fact they have a mobile phone number of their own.

9) SMS messaging is not the most secure method of messaging. Phones can be shared, stolen, and accessed without consent. Any SMS message sent should be brief and contain as little sensitive information as possible.

EMAIL MESSAGING

Email addresses are collected from patients at the time of registration or opportunistically at any time thereafter.

1) Fair processing information will be provided to patients regarding the processing of their email address (the collection and subsequent use).

2) Patients who do not wish to be contacted at all using their email address can either not provide it or ask for it to be subsequently removed from their GP record.

3) Email messaging can **only** be used for the purposes of direct medical care unless the patient has freely given informed, unambiguous, and specific consent to be contacted by email for

non-medical purposes (i.e. direct marketing). Such consent must be recorded and producable in the event of a complaint or audit.

4) Non-medical purposes would be, for example, receiving surgery newsletters, surgery information, minutes of meetings (PPG), Friends and Family Test (anonymous) surveys. etc.

5) All direct marketing emails must include a clear "unsubscribe" message to enable aptients to easily opt-out of this type of email messaging. The simplest way would be to ensure that every such email sent out includes the following line:
"If you no longer wish to receive emails like this from us then please reply to this email, putting "UNSUBSCRIBE" in the subject line. We will then remove you from our mailing list immediately."

6) A suitable consent form is appended to this policy.

Using email for direct medical care

7) Care should be taken to regularly ensure that patients' email addresses are up to date and have not changed.

8) Email messages should contain the minimum sensitive information necessary to achieve the aim.

9) Patients should understand that plain text (i.e. unencrypted) emails are not secure and could be intercepted and read. However the ease of use of plain text emails is very likley to outweigh security considerations for the overwhelming majority of patients.

10) Nevertheless, patients should be aware that emails from the surgery *can* be encrypted if that patient so wants.

11) Encryption can be achieved in a number of ways:

a) If both the sender and the recipient have *public keys* then messaging between them can be encrypted (PGP, GnuPG etc)

b) The NHSmail encryption feature (Trend Micro Encryption Portal) can be used: www.tinyurl.com/NHSencrypt

c) The body of the message can be plain text but attachments (e.g. blood or x-ray results) can be provided as an encrypted PDF (if the sender has appropriate software)

12) No unencrypted patient identifiable data should be transferred electronically across health and social care organisations.

13) If emails are sent from one *@nhs.net* address to another *@nhs.net* address then one can be confident that the content of

the message is encrypted and secure without the need to do anything different.

14) If the email is not *@nhs.net* to *@nhs.net* then the email *must* be secured using the NHSmail encryption feature.

Data Retention

15) Emails to patients should be removed from any "sent" folder as soon as possible and at the latest within one calendar month of the email being sent. Care must be therefore taken to check the contents of email folders regularly to ensure compliance with this.

16) If there is a need to permanently record that email, it should be exported and attached to the patient's GP record.

Complaints

1) Correspondence by email between patients and practice staff in the event of a complaint should be treated as all other emails containing patient identifiable data **–** any such emails should be deleted as soon as possible and no later than 1 calendar month from sending.

2) All such correspondence should be printed off and stored, together with any written correspondence (letter/fax), in a secure storage location.

3) No correspondence about a complaint is to be stored in the patient's GP record.

4) Upon final resolution of the complaint, the file should be kept securely and destroyed **after 3 years** (in line with our data retention policy for such material).

Emailing you for non-medical purposes

We occasionally use your email address to communicate with you about your direct medical care.

We can use email to send you other useful information unrelated to your direct medical care - for example surgery newsletters, surgery information, staff changes, and minutes of patient group meetings - *but only with your explicit consent*.

If you would like to receive this sort of information from us, then please do let us know by ticking the box below.

You can withdraw your consent to receive these type of emails (whilst still allowing the surgery to email you for direct medical care purposes) at any time – just let the surgery know, or email Dr Neil Bhatia (as below).

☐ **Please tick here if you consent to Oakley Health Group contacting you by email with non-medical information (such as surgery newsletters)**

Your name:

Your date of birth:

We never pass your email address on to any third parties (unless you have given us your explicit consent to do so)

Our full privacy policy can be found in the surgery or on our website at www.oakleyhealth.org

If you would like any further information about primary or secondary uses of your GP record, opting out, the NHS Databases, access to your medical record, confidentiality, or about any other aspect of NHS data sharing or your medical records, then please do contact the surgery's Caldicott Guardian / Information Governance lead:
Dr Neil Bhatia
Neil.Bhatia@nhs.net