

EMAIL and Text Message – Communications Policy

Introduction

It is recognised that the use of email and text messaging are well-established methods of communication. Prestige Medical Group supports the use of email and text messaging as a means of communication with patients/service users and carers, subject to compliance with this policy.

2. Scope of policy

This policy sets out the circumstances in which patients, service users and carers can be contacted using email or text message and the procedures that must be followed when using this method of communication.

Responsibilities, accountabilities and duties

This guidance applies and must be adhered to by anyone working within Prestige Medical Group including; but not exclusively, employees, seconded staff and contractors who use or who intend to use text messages and email in the course of their communication with patients and service users.

The Business Manager has overall responsibility for the organisation's data.

The Senior Information Risk Owner is accountable to the GP Partners for information risks and security of information.

The Caldicott Guardian is responsible for the establishment of procedures governing access to, and the use of, person-identifiable information and, where appropriate, the transfer of that information to other bodies.

Managers are responsible for making sure this guidance is highlighted to relevant staff, that it has been understood, and that it is being followed.

Uses

Communication with the Patient community

Example uses of text messages:

Appointment reminders and confirmations

Communicating negative (clear) test results

Asking the patient to call the service at a convenient time

Communicating advice to patient (e.g. bad weather reassurance of a Community Nurse visit)

Ad-hoc communication between key worker and patient.

Example uses of email:

Asking the patient to call the service at a convenient time

Communicating advice to patient (e.g. bad weather reassurance of a Community Nurse visit)

Ad-hoc communication between key worker and patient

Copies of letters sent to GP if requested

Appointment letters.

Justification

Services must individually agree the need/benefit of using email and text message and formally approve and document the implementation of the service. Individual users must not use email or text messages for health-related purposes without formal documented approval.

Local/departmental procedures for the use of email and text message, which comply with this policy, must be documented and cover the following topics:

Identification of the service or facility to be provided

Identification of the need or justification for the use of email/text message

The agreement to the use of the service by its intended beneficiaries/recipients

Clear identification of the associated risks and of the means by which these risks are managed

Storage and retention procedures.

Implied consent

It is appropriate to rely on implied consent when contacting individual patients and service users about their individual care or requesting they complete a friends and family test survey.

It is important that any preferences are recorded in their record and respected. Patients and service users should be able to change their preferences about how they are contacted at any time.

Being open about how information is used

It is essential that the use of email addresses and mobile telephone numbers is in line with transparency guidance and best practice. This means that the use of personal information held by the organisation must be understood by the individual. Services should explain to the patients and service users:

What information they need about them, e.g. mobile number:

For what purpose, e.g. to send appointment reminders;

Who the information may be shared with, e.g. it will not be shared;

What they will do with that information, e.g. it will be stored on your record.

Services should be clear about the rationale for using email and/or text messaging to communicate with their patients/service users and should clearly define the purpose and scope of communication by these means. This includes making patients and service users aware that text messages and emails will not be read during non-working hours and therefore should not be used for urgent queries.

Services should make this information readily available to their patients and service users:

During the registration process

When a mobile phone or email address is recorded/updated

Through online applications, e.g. Patient Online

During contacts with the patient or service user, either in person or on the phone. This doesn't need to be with the clinician and could be with reception staff.

Through information in a waiting area which highlights the benefits to patients and service users and signposts them about how to give their consent.

Children

The age at which a child becomes competent to make certain decisions about their health and care and information sharing will vary depending on the child and the particular decision.

A child with competence is able to make choices about how health and care providers use their information. As such they should be given a choice about who receives emails and messages about their care.

Risks

A Data Protection Impact Assessment (DPIA) must be completed prior to the implementation of the service. In areas where it is felt that risks are unacceptable, the service must not be implemented.

The following risks must always be taken into account:

Confidentiality

Risks can be mitigated to a large extent by only sending non-sensitive messages and by never sending sensitive data such as - "your next ante-natal appointment is..."

Ensuring delivery to the correct recipient

Risks can be mitigated by

Explaining to the patient or service user that it is their responsibility to keep and provide an up to date email address and/or mobile phone number, and to be clear that the service are not responsible for onwards use or transmission of email or text message once it has been received by the patient/service user:

Have processes in place to remind patients and service users to update their email address and mobile number when needed

Contracting out services for sending emails and text messages

If a service wishes to use an external provider, it must seek approval from IG, complete a Data Protection Impact Assessment (DPIA) and ensure all contractual and security measures are in place before any agreement takes place.

Monitoring Compliance

Audit procedures and audit cycles will be established by the IG Team, in collaboration with Operational Services to ensure that:

The exchange of text messages with patients and service users has not created any problems or difficulties for the organisation or for the patient/service users.

Any risks are identified, regularly re-assessed and adequately addressed.

Confidentiality is not put at risk, and that appropriate records of contact are properly maintained.

Any incidents that are raised as a result of email or text message communication with patients and service users will be investigated, reviewed and reported to the [Insert].

Any action required to increase the effectiveness of this policy will be undertaken.

This policy will be regularly reviewed to reflect any changes to national policy, technology or operational practice.

Dissemination

The policy will be available in the complete policy document The policy will also be available on the Organisation's website.