



Cymorth Llywodraethu Gwybodaeth
ar gyfer Gofal Sylfaenol
Information Governance Support
for Primary Care

IGDC • DHCW

IG Guidance for Primary Care Service Providers on Communicating with Patients using the NHS Wales Email Service

Introduction

It is recognised that the use of digital methods to communicate with patients, including the use of email, is increasing. The aim of this guidance is to support the use of NHS Wales email when communicating with patients within a primary care setting.

This guidance is intended for ad-hoc communications on an individual patient basis only. Where an organisation wide change in process is being considered, a Data Protection Impact Assessment must be completed and advice sought from the organisation's Data Protection Officer.

This guidance should be read alongside the [All Wales Email Use Policy for Primary Care Service Providers](#).

Consider the Appropriateness

Users must always evaluate whether the email platform is the most appropriate method to communicate the information concerned. Ad-hoc communications via email should not take place without prior consultation with the patient. It is recognised that it may be the patient's preference to communicate via email, where this is the case, the patient should be informed of the following:

- Emails sent outside of the NHS email domain are not currently considered secure without the use of appropriate safeguards and that whilst the Primary Care Service Provider will use appropriate safeguards when communicating sensitive data, the patient's own emails sent into the organisation may not be secure;
- The patient is responsible for ensuring the correct email address is provided and must inform the organisation of any changes;
- The patient should consider if anyone else has access to the email address (i.e. partner or family), and if so, are they happy for them to see any emails received?

Once this has been explained and they are happy to proceed, the patient's preferences should be documented.

Appropriate Safeguards

Emails sent outside of the @wales.nhs.uk domain, with the exception of those ending @nhs.net or organisations with [Transport Layer Security \(TLS\)](#) enabled, are not considered secure.

Extra safeguards should be used when sharing information by email, these include the use of a file sharing software such as the [NHS Wales Secure File Sharing Portal \(MoveIT\)](#). Where this



is not possible, any documents containing personal information should be encrypted, with no sensitive information and a maximum of two personal identifiers contained within the message body, no personal identifiable information should be contained within the subject heading.

Where encryption is used instead of a secure file sharing software, the password should never be included in the email body and should only be provided once the patient has confirmed receipt of the encrypted document.

One of the largest risks with email is misdirection because of human error. Where possible, copy and paste the email address from a recorded source to avoid mis-typing the email address. When communicating sensitive information, a test email should always be sent first, with the information only provided once the patient has confirmed receipt of the test email. Take your time when emailing personal information, pause and check the email address, email trail and any attachments, and ensure no one other than the patient has accidentally been included in the 'to' or 'cc' fields.

Records Management

The NHS Wales Email system must not to be used as a storage facility. All emails should either be deleted or saved securely to the appropriate record (e.g. to the clinical record).

Any emails that are retained within the email system will be automatically archived by the email system.

Note: At the time of writing, the Email Retention Policy is set for 7 years, with legal hold.

Additional Considerations

Users must maintain an appropriate level of professionalism when communicating by email.

Additional consideration should be given to the tone of the email which could potentially be misinterpreted by the patient. Staff should also be aware that information held on computers, including those held in email accounts, may be subject to requests for information under relevant legislation such as UK General Data Protection Regulation or the Freedom of Information Act.

All staff should be mindful that it may be necessary to conduct a search for information and this may take place with or without the author's knowledge or consent.

