Secure Email Accreditation for Adult Social Care Providers

Contents

What is secure email?

Email is a useful tool for communicating and is excellent for sharing information day to day. But we should be careful about using it to share sensitive information. It can be relatively easy for unwanted people to intercept and access the emails that we send, even when we use strong passwords.

Because health and care information is very sensitive, we must make sure that it is protected. This is true no matter how we send information. Whether using fax, post, email or the phone. This is why email containing health and care information sent to and from health and social care organisations must meet the Secure Email Standard (DCB1596).

How to get secure email?

If you are a CQC registered Adult Social Care Provider in England, there are 2 routes that you can take to ensure your email complies with DCB1596.

1. NHSmail (See Below)
2. Secure email accreditation (See Below)

Which should I choose?

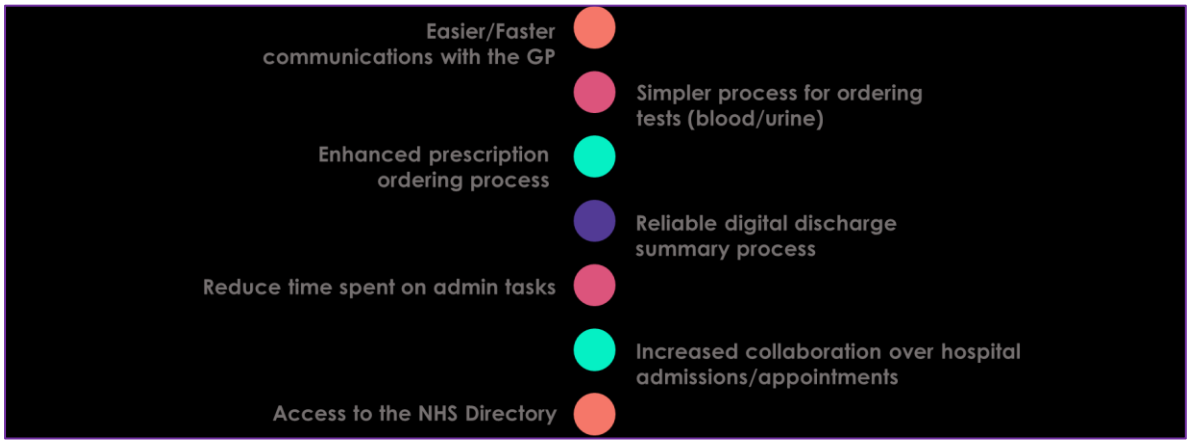
NHSmail	Secure Email Accreditation
Pros: ✓ Free for social care organisations ✓ Instantly recognised as secure across health and care ✓ Access to the NHS Directory ✓ Removes some requirements from the Data Security and Protection Toolkit ✓ Comes with other featues, such as Skype for Business, 4GB mailbox, dedicated Helpdesk support 365 days a year	Pros: ✓ Uses your existing system – no need to retrain staff or change policies ✓ You can keep your existing domain name to maintain brand recognition ✓ Staff do not have to monitor 2 email addresses
Cons: ✘ Only available for staff who need to share health and care information ✘ May require staff to monitor 2 email addresses	Cons: ✘ You will need access to IT support, internally or externally, to complete the accreditation process ✘ Not instantly recognised as secure across health and care

It is up to each organisation to decide which form of secure email you want to use.

NHSmail

NHSmail is a free, secure email system which is available to all providers in England[1] who have achieved Entry Level on the Data Security and Protection Toolkit.

The Benefits of NHSmail



This all contributes to safe and high quality care for those we support.

Access to NHSmail

There are 4 possible routes to NHSmail:-

1. Self-Management (Top Down)

- Suitable for large organisations, i.e. those that have their own IT function, and have the expertise and technological proficiency to carry out the local administrator role
- Organisations manage the accounts themselves – starters, leavers, password resets etc.
- Organisations can integrate NHSmail with their own IT and HR procedures
- The default account allowance is up to 10 user accounts and 1 shared mailbox per site
- Register using the self-management application form. This is completed at HQ level, sites are later added as 'organisation units'

2. National Administration Service (NAS) Portal (Decentralised)

- The main route for small providers, administrative support is provided centrally
- Register via the online self-service portal – usually completed by a care site.

[1] Services provided in Wales and Northern Ireland are not eligible for NHSmail. For Scotland there is a separate application process with different eligibility criteria.

- Nationally administrated, no administrators are required within the social care organisation.
- Dedicated admin support managed via Accenture helpdesk – careadmin@nhs.net
- Generally, the shared mailbox owner for each site manages joiners and leavers. Other responsibilities are detailed in the guide
- Bulk upload facility is available, however there could be a long lead time if large numbers of accounts are required
- May be complicated if the organisation structure is not reflected correctly in the ODS code HQ/site hierarchy (as often seems to be the case)
- The default account allowance is up to 10 named user accounts and 1 shared mailbox per site
- Naming convention for shared mailbox - care.postcodetown.carehomenameODScode@nhs.net (this is being revisited to look at other simpler naming solutions).
- CQC Registered Services only

3. Local Sponsorship.

- Historically this was the only route. Some accounts are already in place, these can be transferred to the National Administration Service
- For care providers who have access to a local NHS trust, clinical commissioning group or commissioning support unit who are willing to sponsor them to join NHSmail. The local sponsor would be required to provide guidance for care providers on joining NHSmail.
- Not normally a viable option for new accounts as local commissioners unlikely to support.

4. Third Party route (For Non CQC Registered Services)

- Separate Application Route – Third Party Process and application form
- Must be providing or supporting publicly funded health and social care.
- The NHSmail team will evaluate eligibility
- Default is up to 50 accounts per organisation

If you would like more information on how to register for NHSmail, please contact us: https://www.digitalsocialcare.co.uk/contact-us/

Secure Email Accreditation

Your organisation may prefer to accredit your existing email system with NHS Digital to demonstrate compliance with the standard. To do this you **must** have:

- An existing Office 365 email service or your own self-managed service (i.e. not a Hotmail/gmail account)
- Access to internal or external IT support
- The ability to provide evidence that you meet the requirements of the standard
- Resources to annually renew your accreditation

If you accredit your system, you will retain your own domain name for your email system. Once the accreditation has been processed, your organisation will be added to NHS Digital's list of accredited organisations.

You can access the current list of DCB1596 accredited organisations here: https://digital.nhs.uk/services/nhsmail/the-secure-email-standard

You may be aware that DCB1596 previously required organisations to change their domain names, i.e. "...@.....secure.nhs.uk". This requirement has now been dropped.

The Accreditation Process

To accredit your system you must follow these steps:

1. Submit a signed self-accreditation statement with evidence. The accreditation statements are available below.
2. Submit the self-accreditation statement and evidence to feedback@nhs.net
3. Have your evidence checked by the NHS Digital Data Security Centre and NHSmail team
4. Rectify any findings and re-submit to the NHSmail team
5. DCB1596 met
6. Renew on an annual basis

Note that the DCB1596 process is completely separate from the Data Security and Protection Toolkit, which will still be a requirement

1. Microsoft Office 365 – accreditation process

If you use Office 365 email, the accreditation process is much simpler than for other self-managed services. You should do the following:

1. Ensure there is a process in place to notify the NHSmail team upon becoming aware of any breach of security, including an actual, potential or attempted breach of, or threat to, the security policy and / or the security of the services or the systems used to provide the services.

2. Have policies and procedures for the use of secure email using mobile devices and ensure the email service enforces them.
3. If applicable to your organisation, comply with the provisions of DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems.
4. Have policies and procedures for staff who use the secure email service to ensure that they understand how to use it appropriately and safely, including how to send emails to insecure email systems (e.g. those used by service users/clients and their friends and relatives)
5. Register compliance with the NHSmail team.

Microsoft Office 365 accreditations **must** include confirmation that the email service has been configured to securely communicate with NHSmail. The Microsoft Office 365: Secure email configuration guide has been co-produced with Microsoft this allows O365 to be enabled to securely route emails to and from NHSmail.

You can download the self-accreditation template from the secure accreditation page: https://digital.nhs.uk/services/nhsmail/the-secure-email-standard

2. Exchange, hybrid or other email services

If you are using an email system other than Office 365 you must complete the Organisation section of the standard and **also** submit assertions and evidence that they meet the ICT Service Provider elements of the standard.

The templates for this can be downloaded from the secure accreditation page: https://digital.nhs.uk/services/nhsmail/the-secure-email-standard

3. What to do once you have achieved accreditation

Once accredited, your domain will be added to the NHS Digital list of DCB1596 accredited organisations. This means that NHSmail users can be assured that emails sent between your addresses and NHSmail are secure.

However, in practice, most users will not be aware of the list of DCB1596 accredited organisations, and so may not immediately recognise your email as secure. Therefore you should also have conversations with the partners that you regularly share information with, to explain to them that your email domain is accredited. You can encourage them to add the NHS Digital list of accredited organisations to their internal email whitelists (this will also be happening for NHSmail in the near future).

You can use the list to apply your own transport rules such as to invoke local message based encryption tool for non-accredited domains or create your own Mail Tips.

You will have to implement a policy on how frequently you will update your own Whitelist as organisations will be added and removed throughout the year.

4. Re-accreditation

Your accreditation will last one calendar year. After this, you will need to reaccredit your organisation.

Reaccreditation requires you to resubmit evidence for review. Generally, this will be similar to what you have previously had to submit. Penetration test results and ISO27001 certificates must be within the last 12 months.

It is your responsibility to ensure that your organisation re-accredits every year.

Additional information

You can access statements on how NHSmail and Office 365 comply with email security obligations from the secure accreditation page:
https://digital.nhs.uk/services/nhsmail/the-secure-email-standard

Communications

Providers are strongly encouraged to communicate their strategy regarding NHSmail/secure email to all sites/branches, so that when approached by local commissioners they can respond accordingly. In particular, they should be made aware of your policy regarding individual NHSmail applications via the NAS, as commissioners will often encourage providers to do this.

Help!

If you would like to discuss secure email accreditation or NHSmail with NHS Digital, please contact the NHSmail team on feedback@nhs.net. You will receive a response within 5 working days.