

Welcome to the NHSmail LA webinar

- The webinar will begin at 11am.
- Please synchronise your web and phone presence by inputting your **Attendee ID** into the phone.
- Participant lines will be muted during the presentation.
- The webinar will be recorded.
- You can use the chat messaging feature on the right of the screen to ask questions. Please only use this for questions, not general comments.

NHSmail Local Administrator webinar

Wednesday 28 March 2018 at 11am

Agenda

- Service status
- Account management lifecycle
- Application accounts
- Business continuity and disaster recovery testing
- Anti-spoofing
- Skype for Business – file sharing and recording
- Growth areas
- Questions

Service status

Update on NHSmail service

Tom Blackmore, Service Management Lead, Accenture

Service status

- Service across the NHSmail platform remains consistent with previous months.
- There was a high severity service incident (HSSI) raised earlier in March relating to NHSmail Relay delivery delays, but this was a minor issue and quickly resolved.
- Self-service password reset take-up has risen again during February 2018. However, usage of this functionality remains at a modest 14.5% of total password resets conducted on the platform - this is compared with 82.5% carried out by Local Administrators.

Account Management Lifecycle

- Further to the information provided in the previous webinar, we are intending to deploy functionality that will automatically manage the lifecycle of NHSmail accounts in line with the Information Management Policy.
- The automated process will not be switched on until piloting has taken place. We will communicate further on timescales.
- In the meantime, the NHSmail team will be undertaking further manual activities in preparation:

Leaver accounts

- During early April 2018, we intend to remove a batch of accounts that have been a 'Leaver' beyond the 30-day period documented in the Information Management Policy.
- The intention to delete the accounts will be supported with communications directly to the mailboxes in scope, at least 14 days in advance. This will allow time for any corrective actions to be taken to prevent deletion due to accounts being in the wrong status.

Inactive accounts

- It is expected that further manual deletion activities will be carried out focusing again on 'Inactive' users, during the end of April 2018 and beginning of May 2018.

Application Accounts

- If a mailbox is used for sending a high volume of emails, it can be converted into an 'application account'.
- Different policies apply to an application account:
 - Passwords are required to be more complex (20 characters with a mix of upper / lower case characters, and a number or symbol).
 - The interval between password resets is 12 months.
 - Deleted emails are not recoverable once the 'deleted items' folder is emptied.
- If a mailbox needs to be converted from a personal (user) mailbox into an application account, it must be appropriately named to indicate that it is being used for sending high volumes of emails as part of a business process, for example: appointment.reminder@nhs.net.
- Existing shared mailboxes cannot be converted to application accounts.
- Upon conversion to an application account, the account will require a password change immediately irrespective of whether the existing password meets the complexity requirement.
- If you wish to convert a mailbox to an application account, please contact feedback@nhs.net.

Business Continuity and Disaster Recovery (BCDR) Testing

- The next BCDR test is scheduled for 21 September 2018 and is due to run until 30 September 2018.
- We do not expect any impact on end users during the course of the test and further communications with more details will be issued in advance.
- However, it would be appreciated if LAs would ensure that local business continuity arrangements are reviewed as a precaution.
- In addition, if organisations / boards are involved in self-migration activity to NHSmail please plan in a pause of this activity over the course of the BCDR testing period.

Questions?

Anti-spoofing

Tom Blackmore, Service Management Lead, Accenture

Anti-spoofing

What is spoofing?

- Sending emails via applications using an internet-based email domain, giving the appearance that the email has been sent from an @nhs.net email address.

Approach to switching off the ability to spoof

- To protect the NHSmail service, the practice of spoofing @nhs.net addresses will be prevented later this year. All email will need to either be sent from @nhs.net accounts, or into the NHSmail service from external sources without spoofing an @nhs.net email address.
- The first change to be implemented will be that, for a period of time to be confirmed, any emails spoofing @nhs.net will be directed to a user's 'junk' mailbox.
- Following the above period of time, the second change to be implemented will be that any emails spoofing @nhs.net will be deleted from the NHSmail service and will not be delivered to a user's account.
- Timescales for these changes will be communicated in due course.

Anti-spoofing

Enabling SMTP / POP / IMAP over the internet

- Currently, functionality enabling the use of SMTP / POP / IMAP connections over the internet is not enabled and this means that organisations are unable to send with an NHSmail email account over the internet without spoofing.
- New functionality is due to go live in April 2018 (guidance on enabling user accounts to use SMTP / POP / IMAP over the internet will be made available prior to go live). These organisations will then be able to request an NHSmail account (or use one they currently have correctly) and legitimately send emails from nhs.net, rather than spoofing @nhs.net.

Solutions

- Use an @nhs.net account to send emails over the internet once the SMTP / POP / IMAP functionality is available.
- Continue to send emails from the external email domain using the proper name, without spoofing @nhs.net.

Anti-spoofing

Next steps (pending SMTP / POP / IMAP functionality going live)

- Identify any users that are spoofing @nhs.net or receiving emails that are spoofing @nhs.net.

Emails that spoof @nhs.net addresses are already tagged as follows:

--- This message was sent from an email address external to NHSmail but gives the appearance of being from an NHSmail address. Verify the sender and content is legitimate before acting upon information contained within. ---

- Anyone requiring the use of an NHSmail account, to avoid spoofing, should set one up in preparation for the change on the service later this year – the account must remain ‘active’.

Questions?

General service information

**Dayam McIntosh, Project Manager,
Growth & Data, NHS Digital**

Skype for Business – file sharing and recording

- File sharing – available to all organisations currently using Skype for Business Instant Messaging and Presence on NHSmail.
- Recording – available to those organisations using Skype for Business Audio and Video Conferencing as an additional service.
- To arrange for either of these to be switched on, email feedback@nhs.net.

Growth Areas

- Pharmacy
 - Accounts currently owned by organisations other than the central NHS Pharmacy container are in the process of being moved. You may receive queries for any that are owned by your organisation – please assist with marking accounts as ‘Leavers’ if requested.
- Dentistry and social care organisations
 - We are planning pilots with dentists in London and social care organisations, during April 2018, for the use of NHSmail.
- Optometry and locums / transient workers
 - Pilots are planned for summer / autumn 2018.

Questions?

www.digital.nhs.uk

 [@nhsdigital](https://twitter.com/nhsdigital)

enquiries@nhsdigital.nhs.uk

0300 303 5678