Document filename: NHSmail2 Requirements 1.9			
Directorate / Programme	National Applications	**Project**	NHSmail 2
Document Reference			
Programme Manager	Jon Calpin	**Status**	Draft
Owner	Clive Star	**Version**	1.9
Author	Steve Gore	**Version issue date**	26/04/2013

NHSmail2 Requirements

Document Management

Revision History

Version	Date	Summary of Changes
0.5		For internal review
0.7	20/11/2012	Major revision incorporating the following: • Review comments from v0.5 of this document. • Requirements from "NHSmail 2 Initial User Engagement v0.5". • User feedback sent to the NHSmail 2 mailbox. • User feedback posted on the NHS Networks site.
0.8	05/12/2012	Major revision incorporating the following: • Review comments from v0.7 of this document. • All detailed requirements, mostly from "NHSmail 2 Initial User Engagement", are now in another document "NHSmail 2 Requirements Change Log". • More user feedback sent to the NHSmail 2 mailbox. • More user feedback posted on the NHS Networks site.
0.9	19/12/2012	Major revision incorporating the following: • Review comments from v0.8 of this document. • More user feedback sent to the NHSmail 2 mailbox. • More user feedback posted on the NHS Networks site.
1.0	20/12/2012	Minor changes. Up-issued and approved for release.
1.1	10/01/2103	Minor changes to clarify requirements.
1.2	10/01/2013	Minor changes to clarify requirements.
1.3	11/01/2013	Up-issued and approved for release.
1.4	23/01/2013	Changes from review comments and supplier workshops.
1.5	30/01/2013	Major document re-structure, now split into individual components and common components. Some requirements reworded and/or moved between sections.
1.6	12/02/2013	Up-issued and approved for release.
1.7	12/03/2013	Minor updates, for internal review (including by User Council as part of validation process)
1.8	28/03/2013	Simplified service management section. Added in essential criteria. Added nhs.uk relay.
1.8a		Interim update to reflect Fax at IL3 instead of IL2
1.9	26/04/2013	Clarifications added to a number of sections to help suppliers understand NHS context better Security requirements updated to reflect security risk assessment

Reviewers

This document must be reviewed by the following people: author to indicate reviewers

Reviewer name	Title / Responsibility	Date	Version
User Council			
Supplier Council			
NHSmail 2 Project team			

Approved by

This document must be approved by the following people: author to indicate approvers

Name	Signature	Title	Date	Version
NHSmail 2 Programme Board		NHSmail 2 Programme Director		1.9

Glossary of Terms

Term / Abbreviation	What it stands for
Active Session	The period during which a User is logged on to the Services, determined from the moment when the User's credentials are authenticated by the Services until the moment when that User ceases to use the Services by either logging out or, after an agreed period of inactivity, the User is automatically logged out for security reasons.
Administrator	A User who has access to special tools to administer User accounts and other aspects of the Services received by their Organisation or group of Organisations.
Anonymous User	A User who has not authenticated themselves to the Services using authentication credentials such as to access the directory or training/guidance material from a secure network.
Archiving Service	A service to enable each User to archive their own email and/or calendar data.
Automatic Password Reset	Functionality which enables a User to reset their password through the supply of several factors known only to that User.

Document Control:

The controlled copy of this document is maintained in the HSCIC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1 Overview

1.1 Vision

Information is the lifeblood of health and care, but is only useful if available to the right person in the right place, at the right time. Patient records are the primary source of clinically rich information for Healthcare Professionals, but clinical information needs to be shared, and in a variety of different ways. A fundamental way to share information is by email.

In addition to email, the way that individuals share information has changed significantly over the past decade, adopting instant messaging, cloud storage, web conferencing, video messaging, and other technologies. There are real opportunities for health and care to take the best of this technology and mould it to its own needs.

The investment will satisfy the following business objectives:

Information Sharing

The Information Strategy, 'The Power of Information' (May 2012) sets out that health and care information will flow freely, safely and securely around the system to the right person, in the right place at the right time. It will not be constrained by organisation or care setting boundaries. The replacement for NHSmail will allow communication and data exchange between health and care users and their patients as part of this infrastructure.

Best Value

The public sector uses its substantial buying power to effectively and in a joined up fashion negotiate the best value for money when it buys a service.

Technology That Just Works

Consumer technology has set the expectation that it just works. This is a fundamental aspiration for the new service.

1.2 Current Situation

In December 2012 NHSmail had a total of 931,935 registered mailboxes and generic accounts with 528,812 person accounts in regular (daily) use within the NHS of which 80,000 were in Scotland. 152 organisations and many thousands of GP Practices use it as their sole email service, with another 341 organisations using it to a greater or lesser extent. NHSmail and the @nhs.net email domain are trusted throughout the NHS and government services as a secure email system.

The system currently comprises email, calendaring, directory, email hygiene (spam and malware protection), SMS, fax, monitoring, and a mail relay service to connect non-NHSmail users. It is an email service through which NHSmail sender and receiver can be assured that information is secured in the creation, delivery and receipt of the message.

The service continues to grow, with an average growth of 16,524 new accounts each month in 2012 and many new organisations in the pipeline. The service also sends between 10 million and 14 million SMS text fragments per month. The usage is growing each month.

1.3 Requirements

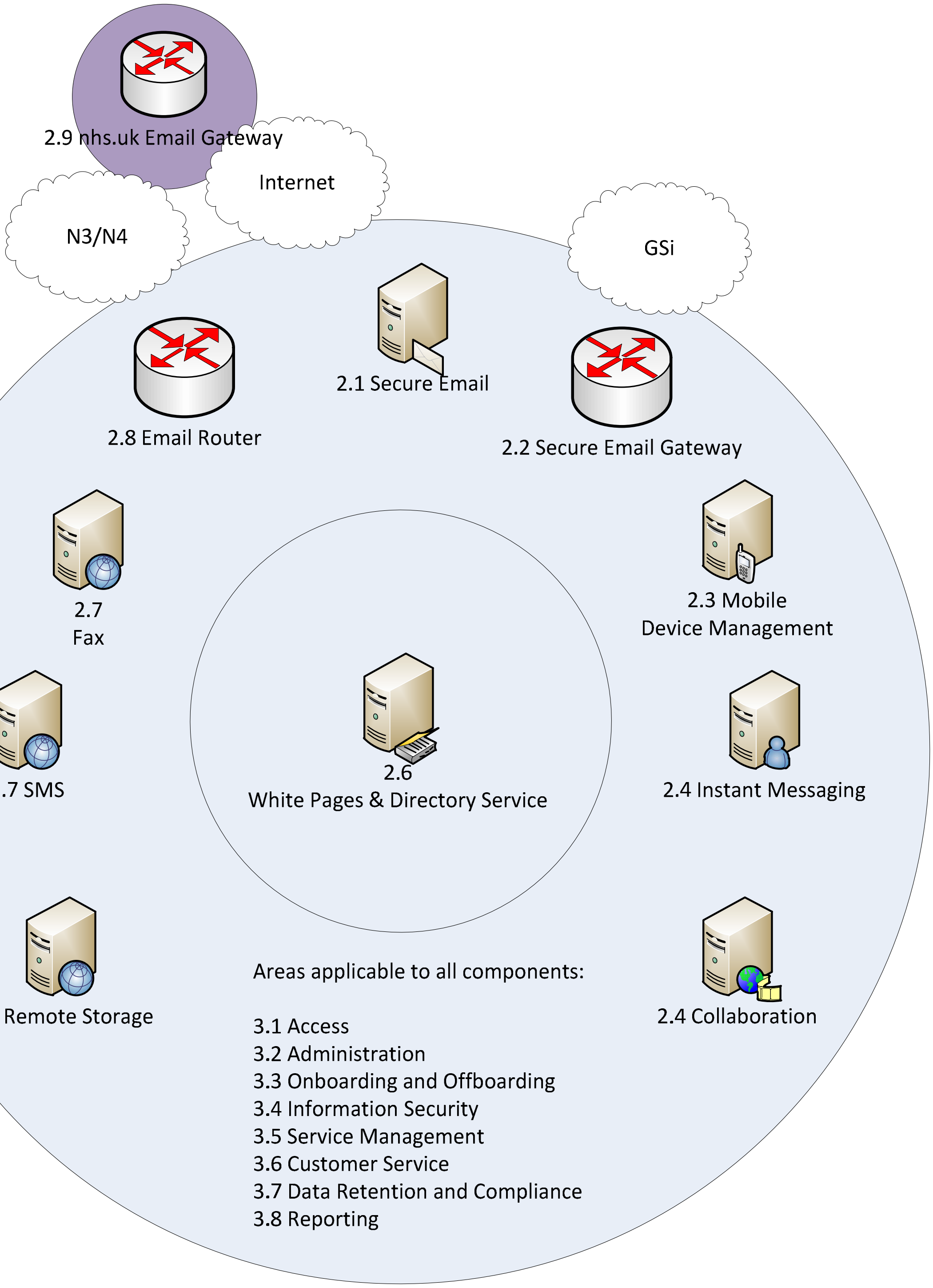
The requirements are broken down into two sections:

- Individual Components
- Common Components

The individual components have been broken down to open up the opportunity for small and large service providers to provide solutions and services. Some suppliers may therefore find that they have a commodity product that is able to fulfil the requirements of a number of the individual components e.g. Secure Email, Secure Email Relay and Mobile Device Management.

The common components describe the areas that apply in full to each individual component.

If every component was provided by a different supplier the service could be represented as follows:



Areas applicable to all components:

3.1 Access
3.2 Administration
3.3 Onboarding and Offboarding
3.4 Information Security
3.5 Service Management
3.6 Customer Service
3.7 Data Retention and Compliance
3.8 Reporting

2 Individual Components

The following components are all individual components of the service. Each of these individual components is accompanied by all of the common components in Section 3 below.

2.1 Secure Email

2.1.1 Vision

Secure Email

Health and care staff will have access to secure, reliable email that allows them to safely share emails containing confidential patient information within the @nhs.net domain, and also with other parties outside the domain. (For example: patients, health and social care, the police, social services, law firms, etc). The email service should integrate with email clients on a wide variety of end user devices. It should be available both on and offline and give safe ubiquitous (internet) access.

The email services offered will be selected by and appropriate to health and care organisations and users. This may mean that some users have access to email using a mail client on a PC; others will prefer browser-based access or mobile device access, whilst the remainder will prefer a full groupware service. One size does not fit all. The service will also need to support application integration so that local healthcare applications can leverage the service.

Email Address for Life and Local Email Address

Every account is provided with an email address for their life in the NHS to support re-organisation, organisation transfer and transitional assignments (national address).

Email addresses containing organisation name are critical to health and care organisations who value and/or rely on their branding. All users should have a @nhs.net email address for life, as is the case now, but also have the ability to have an alias containing the local organisational abbreviation (local email address) that all deliver to the same mailbox. For example: john.smith@nhs.net as the email address for life, and john.smith@examplehospital.nhs.net as an alias.

If John Smith moved organisations at some point, john.smith@nhs.net would continue to work, john.smith@examplehospital.nhs.net would be deactivated and a new alias for the new organisation would be created.

Generic email addresses (medical.director@examplehospital.nhs.net) will be permitted, and can be transferred between users as people start and leave positions.

Over time organisations will be renamed or merge. The user will build up a history of email address aliases but the service will manage this ensuring email is only delivered to the active addresses with configurable behaviour on email sent to a deactivated email address.

2.1.2 Current Situation

The current service uses Microsoft Exchange 2007 at its core, with a customised web application to provide the entire additional web based components. The portal does not provide a customised version of Outlook Web Access although it does through Outlook Web Access Web Parts provide access to mailbox folders and delegation. Two-thirds of users access their email primarily via the web browser.

2.1.3 Requirements

#	Requirement	Essential
Email		
1	The email service must provide email across health and care organisations using the @nhs.net domain which will contain sub domains. The service must support the inclusion of additional secure domains should other organisations wish to bring their own secure domain e.g. organisation.hsi.gov.uk , The email service must route email to and from the internet, to and from the nhs.uk domain and SMS/fax gateways.	Y
2	The email service must provide two types of account: • Personal. • Generic: o Shared generic accounts. o Resource accounts (e.g. room bookings) o System accounts (e.g. for applications that send emails)	Y
3	The email service must provide industry standard email functionality, such as: Reports for delivery and non-delivery of emails, an out of office message facility, and automatic forwarding (only to approved secure domains).	Y
Delegation and Sharing		
4	The email service must provide the ability to share, and delegate access to, an account's email, calendar, tasks, and contacts with other users of the service whether in the same Organisation or another Organisation. In the case of personal accounts, this functionality should only be available to the user who is the owner. In the case of generic (i.e. shared) accounts, this functionality should be available to the account's owner(s).	Y
Distribution Lists		
5	The email service must provide tools for users to create and manage centralised static and dynamic distribution lists based on local and central directory information that are available to all users of the service. Dynamic distribution lists should be able to leverage the fields of the directory service e.g. all Nurses in a Clinical Commissioning Group working in Paediatrics.	Y
6	The email service must provide tools for users to create and manage personal email distribution lists that are available only to themselves.	Y
Quota and Archiving		
7	The email service must provide an account quota per user for each and every account in an organisation, for both personal and generic accounts. This must include and be shared between emails, calendar appointments, tasks, and contacts.	Y

8	Suppliers should give organisations the option of purchasing larger quotas, for both personal accounts and generic accounts.	
9	The email service should provide an archiving solution that is seamlessly integrated with the email service and completely transparent to users.	
Integration		
10	The email service Supplier must integrate with any other components of the service that deliver the overall capability.	Y
Email Address for Life		
11	All users must have a @nhs.net email address for life and the ability to have an alias containing the organisational abbreviation that all deliver to the same mailbox. For example: john.smith@nhs.net as the primary email address, and john.smith@examplehospital.nhs.net as the alias. If John Smith moved organisations at some point, john.smith@nhs.net would continue to work, john.smith@examplehospital.nhs.net would be de-activated and a new alias for the new organisation would be created by automated workflow based on the properties of the account in the directory. This is necessary because there is no national work flow that tracks a user moving from one organisation to another. The Organisation should have the ability to set the default reply address at a per account level for both personal and generic accounts. Over time organisations will be renamed or merge and users may change their name. The user will build up a history of email address aliases but the service will manage this ensuring email is only delivered to the active addresses with configurable behaviour on email sent to a deactivated email address	Y
Search		
12	The email service should provide an overarching search function that searches all parts of a user’s account (email, contacts, tasks, calendar, etc.) in a single search.	
13	The service must allow a user to enter advanced search criteria such as narrowing the time/date range of the search, specifying a particular sender, or limiting the search to an individual part of a user’s account such as email or calendar only.	Y
Email Hygiene		
14	The email service must provide industry leading anti-virus and anti-spam filtering. In addition to commodity content management such as attachment blocking, virus/spam filtering capabilities and data leakage prevention there should also exist options for managing spoofed/forged email and items that cannot be checked such as S/MIME encrypted or password protected attachments.	Y

2.2 Secure Email Gateway

2.2.1 Outcome

There will be a central email gateway between other secure email services (specifically GSi) and NHSmail 2. It will also provide a secure capability to send bulk email from applications and an email encryption gateway.

The Secure Email Gateway typically aligns with the capabilities commodity email gateways, anti-virus/anti-spam products, mail hygiene services, email filtering services, relay services and email encryption services.

2.2.2 Current Situation

There is currently a central gateway between NHSmail and GSi which securely transmits small volumes of email. Exchanging sensitive email to insecure email addresses such as internet or nhs.uk recipients is currently achieved via S/MIME which is both cumbersome and difficult to use and identified by users as an area needing improvement.

2.2.3 Requirements

#	Requirement	Essential
1	The Email Gateway must transfer email messages securely between the email service and: • The Government Secure Intranet (*.gsi.gov.uk, *.gsx.gov.uk, *.gse.gov.uk, • Secure email domains in Local Government/Social Services (*.gcsx.gov.uk) • Criminal Justice/Police National Network (*.pnn.police.uk, *.scn.gov.uk, *.cjsm.net). • Secure email domains in the Ministry of Defence (*.mod.uk) • Other networks or organisations as from time to time specified by the Customer.	Y
2	The Email Gateway must provide a lightweight relay service for bulk emails. This must not support email services outside the nhs.net domain.	Y
3	The Email Gateway must provide: • SMTP authentication. • Encryption of data in transit to and from the gateway. • Access from authorised IP addresses	Y
4	The Email Gateway must provide non-delivery reports for email messages which are unable to be delivered by it.	Y
5	The Email Gateway must contain functionality to support secure MIME standards.	Y
Email Hygiene		
6	The email service must provide industry leading anti-virus and anti-spam filtering. In addition to commodity content management such as attachment blocking, virus/spam filtering capabilities and data leakage prevention there should also exist options for managing spoofed/forged email and items that cannot be checked such as S/MIME encrypted or password protected	Y

	attachments.	
Security		
7	The email service must provide bi-directional user friendly email encryption (including attachments) to any insecure email addresses. This is to support email exchange to Organisations and individuals operating outside of the secure email domains provided for in requirement 1 of this section. This method of encrypting content should support both configurable automated and manual methods e.g. encrypting based on content and user action. Encryption/de-encryption should not prevent data being searched/discovered for compliance purposes.	Y

2.3 Mobile Device Management

2.3.1 Outcome

Mobile device access is becoming the primary method of accessing NHSmail accounts for many users. For others, it is their secondary method but is critical when away from their desks or the office. Therefore, compatibility and support for a wide range of mobile operating systems and devices is critical, especially for organisations operating or considering a BYOD (Bring Your Own Device) arrangement with their users. Enforcement of the mobile device policy is critical too, for the security of the service and the confidentiality of patient information.

This requirement is primarily about protecting the data a user could hold on their device from any component of the service. Any additional management capabilities will of course be welcomed but they are not essential for the replacement service.

Organisations are particularly keen to prevent devices that have been rooted or ‘jailbroken’ from connecting to the service or devices that do not meet the minimum security requirements.

2.3.2 Current Situation

Email services are accessed using a variety of mobile devices via the Exchange ActiveSync protocol only. Blackberry devices are used with an Exchange ActiveSync client and not through Blackberry Enterprise/Internet services.

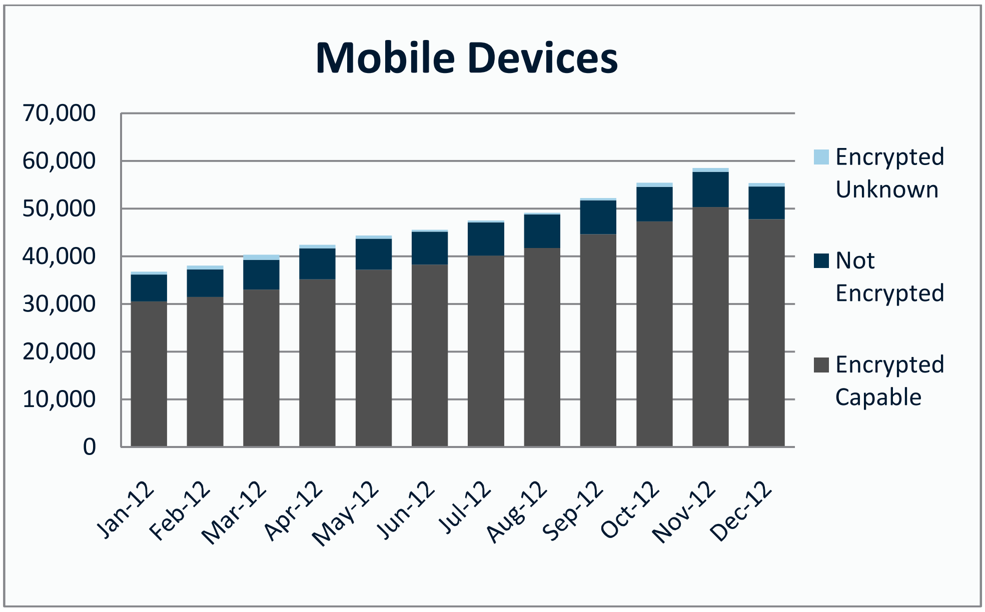
A range of standard mobile device policies are applied to minimise the risk of data loss and data aggregation such as requesting device encryption, requiring a device password and limiting the amount of data that can be sent/received to 30 days of email and messages up to 500 KB

There is currently no restriction on types of mobile operating system or devices. The table below gives the breakdown of usage in December 2012:

Device Type	Percentage
iPhone	57%
iPad	20%

Android	12%
Blackberry	4%
Nokia	4%
Windows	3%

Usage of mobile devices is small but growing over time.



2.3.3 Requirements

#	Requirement	Essential
1	The service must support the most popular mobile/tablet device operating systems. As a minimum: • Apple iOS. • Android. • Windows RT. • Windows Phone. • BlackBerry OS. • Nokia (Symbian).	Y
2	The service must remotely enforce the Customer's mobile device policy on all devices, and must reject any device that: • Does not meet the minimum security requirements. • Does not enforce the minimum security requirements. • Does not report to the email service on either of the above.	Y
3	The email service must provide organisation administrators with a Mobile Device Management capability, to manage all of an organisation's mobile devices remotely, including: • Central and local policies (local policy cannot override central policy). • Functions to allow/deny/quarantine by device type, organisation or groups of users.	Y

	• Remove device, expire password, and wipe any data associated with the service. • Reporting functions/ capabilities. • Detect and block rooted (i.e. jail broken) devices.	
4	A fully featured mobile device management capability to provide additional functionality over and above that required for the NHSmail service may be offered as a locally funded ‘top up’ service.	

2.4 Instant Messaging and Collaboration

2.4.1 Outcome

Users across health and care have access to an instant messaging and collaboration solution that just works, and includes:

- Instant messaging.
- Audio conferencing.
- Video conferencing.
- Shared workspaces, documents, and device desktops.
- VoIP (Voice over Internet Protocol) integration.

This may be delivered within an email service or alongside it.

Suppliers should comply with open standards to ensure seamless integration between services.

Suppliers should recognise the need for users to have a different availability status e.g. appearing ‘available’ to all staff in their Organisation, ‘available’ to some staff in another Organisation and ‘not available’ to all other NHSmail users.

Suppliers should recognise the need to collaborate beyond the service.

2.4.2 Current Situation

Each health and care organisation has chosen its own instant messaging solution, or chosen not to have one. Some organisations have bought their own conferencing facilities, especially for uses such as MDT (Multi-Disciplinary Team) meetings. In many cases there is no integration between organisations or indeed different vendor solutions.

2.4.3 Requirements

#	Requirement	Essential
1	The instant messaging and collaboration solution should include: • Instant messaging. • Audio conferencing. • Video conferencing. • Shared workspaces / documents. • VoIP (Voice over Internet Protocol) integration.	
2	The service should work across health and care organisations, and integrate with the relevant service components.	
3	The solution should integrate with the directory service. It should provide directory information on its users and organisations to the directory service. It should use the directory service to look up email addresses, distribution lists, phone numbers, and other entities.	
4	The solution should provide shared spaces for users during a conversation, such as shared whiteboards, shared documents, and shared device	

	desktops.	
5	The solution may, where safely available and where possible, provide interoperability with other instant messaging and collaboration solutions.	
Content Protection		
6	The instant messaging and collaboration service must provide industry leading anti-virus protection. In addition to commodity content management such as attachment blocking and virus detection there should also exist options for data leakage prevention and items that cannot be checked such as password protected attachments.	Y

2.5 Remote Storage

2.5.1 Outcome

Health and care users will be able to store and share documents in a secure manner. The service will ensure that they are not infected by viruses or other malware. Health and care organisations will be able to manage the remote storage of their users to ensure they are used appropriately; manage quotas, comply with access requests, etc.

2.5.2 Current Situation

There is no central remote storage service.

2.5.3 Requirements

#	Requirement	Essential
1	The remote storage service should allow users to store and retrieve files from their own personal area. This will have ubiquitous access.	
2	The remote storage service should allow users to share files with other named users, groups, or everyone. The users and groups will be determined by entries in the directory.	
3	The remote storage service should seamlessly integrate into other applications (including the operating system) through the use of standards-based methods.	
4	The remote storage service should allow shared working on documents, spreadsheets, etc.	
Administration		
5	Administrators in User organisations should be able to: - Manage user remote storage accounts (e.g. create, suspend, delete, password reset). - Assign different quota sizes to individual users, groups of users, or the whole organisation - Remove user accounts, including detecting and removing duplicate and inactive accounts. - Transfer users between organisations within the same Supplier. The transfer of users between Suppliers is managed separately. - Recover files from a user’s remote storage area. - Monitor usage, including serving regulatory requests (e.g. Freedom of Information).	

Search		
6	The service should provide a search function that searches all parts of a user's account in a single search.	
7	The service should allow a user to enter advanced search criteria such as narrowing the time/date range of the search or specifying a particular file name.	
Content Protection		
8	The remote storage service must provide industry leading anti-virus protection. In addition to commodity content management such as attachment blocking and virus detection there should also exist options for data leakage prevention and items that cannot be checked such as password protected attachments.	Y

2.6 White Pages & Directory Service

2.6.1 Outcome

Health and care covers a vast range of organisations and a large number of staff in the public and private sector. Good quality care depends upon finding the correct person and communicating with them. A central White Pages has the ability to help deliver this as long as it is trusted, accurate and up to date. The directory and white pages provides contact details for people in all NHS organisations, not just nhs.net email users.

Users will be able to find contact information for a user, group or organisation. This should cover all aspect of communication, for example address, phone number, teleconferencing details. They will have access to features now standard in social networks, for example a photograph, status and location, with appropriate security controls around this.

The White Pages should be maintained by authoritative data sources with organisations able to select a combination of system and self-service updating dependant on their local approach to data management. There will be appropriate tools to ensure that data quality and consistency is maintained, with local administrators being able to easily operate on a large number of entries.

Consideration needs to be given to segmentation approaches in the event of the service being used by non-health and care organisations. This will be considered when evaluation role based access controls.

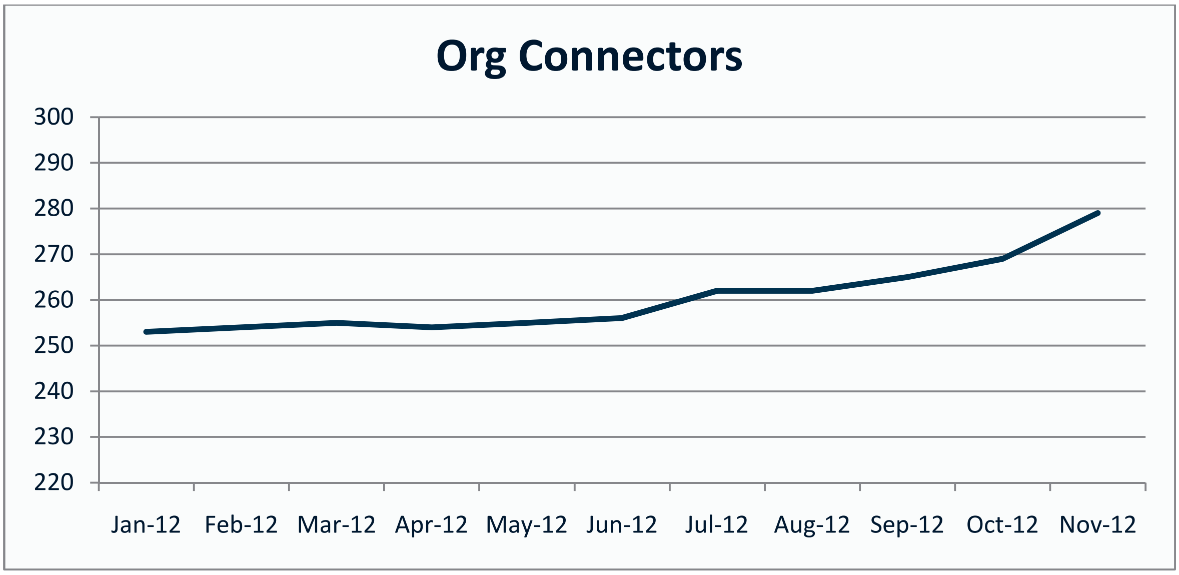
2.6.2 Current Situation

There are a large number of directories that identify users and their contact information:

- Spine Directory Services (using smart cards for access control).
- Electronic Staff Record.
- NHSmail directory.
- Local directories.

Whilst many of these share information between them there is not a single consolidated view of contact information.

Local organisations are able to use connectors to provide manual and automatic updates to the current directory. The graph below shows the total number from Jan 2012 to Nov 2012.



2.6.3 Requirements

1.5	Requirement	Essential
Content		
1	The Directory Service must provide a directory of people (health and social care staff members), organisations, distribution lists, and generic mailboxes.	Y
2	The Directory Service must provide contact information for each of the entities useful for health and care and necessary to support the national NHS network and email services.	Y
3	The Directory Service must be for use by and contain information on all health and care organisations, not just those using NHSmail.	Y
4	The Directory Service may cater for users who work for more than one organisation, making it clear that they are a single person working in multiple organisations.	
Access		
5	The Directory Service must be accessible by all health and care staff (public and private and third sector) and other public sector staff through role and location based access controls. It must not be publicly available on the internet.	Y
Administration		
6	The Directory Service must support an extensible schema to allow additional attributes to be added for users.	Y
7	The Directory Service must support the Customer’s organisation hierarchy and be sufficiently flexible to accommodate regular restructuring.	Y
8	The Directory Service must allow users to update elements of their individual entries where permitted by their organisation.	Y
9	The Directory Service must allow administrators to maintain data quality on both individual entries and in bulk. The Directory Service must support administrators to maintain data quality.	Y
Integration		
10	Health and care has a number of national directory services, for example the Electronic Staff Record and Spine. Local organisations will have others. Still	Y

	more may be provided by the Public Services Network. The Directory Service must integrate with these directories through industry standard interfaces. Authoritative updating of fields will be on a per Organisation basis from nominated authoritative data sources.	
11	The Directory Service must provide the ability for local health and care organisations to query the directory using standards-based methods.	Y
Migration		
12	The Directory Service must seamlessly take over from the existing NHSmail directory	Y
Search		
13	The Directory Service must provide a powerful advanced search and browse function, with the ability to search (and filter search results) by organisation, role and other criteria.	Y

2.7 SMS & Fax Gateways

2.7.1 Outcome

Users will be able to send and receive emails that convert to SMS text messages and faxes. The gateway will benefit from the large volumes of SMS text messages and faxes sent by health and care but give user organisations individual control.

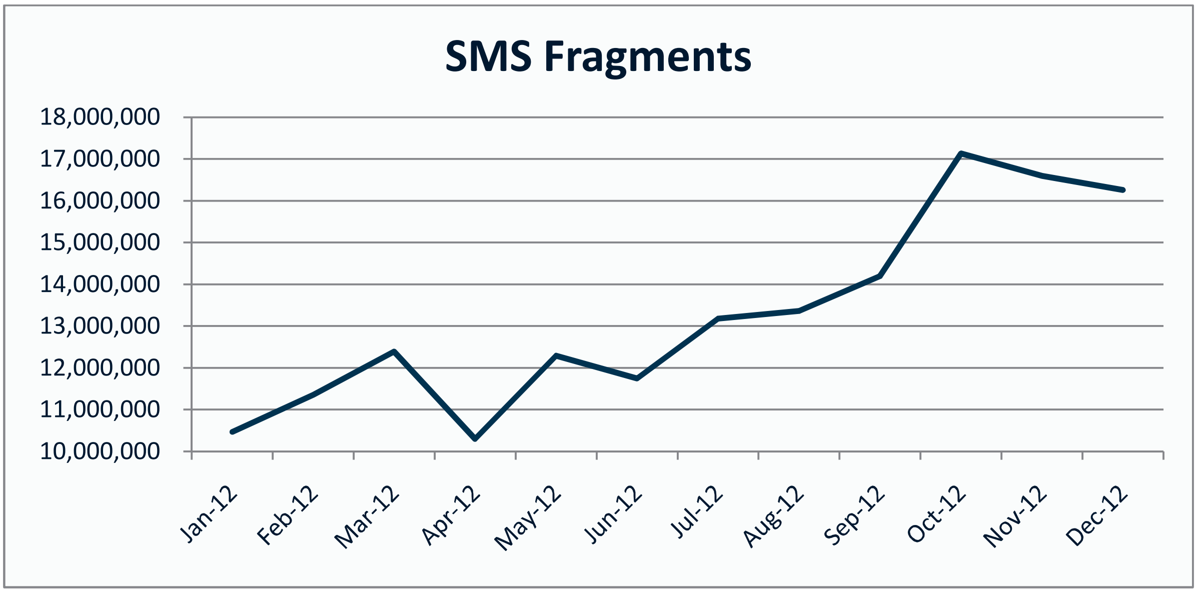
Capacity will, in due course, be bought by individual health and care organisations based upon their needs. The intention is that individual organisations will be charged based upon their usage but receive the volume discount price for health and care. The Customer will receive information on total usage so it can assess value for money.

2.7.2 Current Situation

The current service provides an SMS and fax gateway which is well used. It is anticipated that usage will increase if the service is made more widely available. Currently it is not marketed due to capacity and cost concerns.

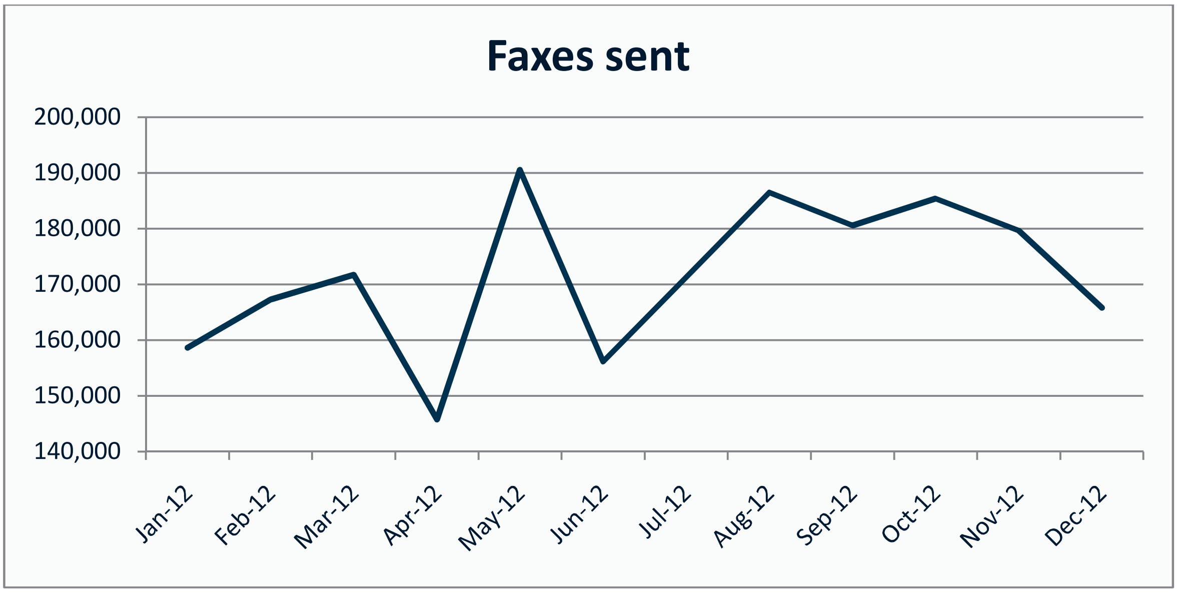
SMS

The current NHSmail service provides an outbound email to SMS gateway, although there is a demand for an inbound service. The graph below shows the uptake of the service.



Fax

The current NHSmail service provides an outbound email to Fax gateway. The graph below shows the volumes per month.



2.7.3 Requirements

#	Requirement	Essential
SMS Gateway		
1	The SMS Gateway must provide an SMS service for inbound and outbound messages that integrates with the email service.	Y
2	The SMS Gateway must contain functionality which: • Validates SMS content and size before sending. • Encrypts user data in transit to the entry point to the mobile network. • Provides keyword routing to enable a single message short code to be used for multiple tasks. • Provides non-delivery and delivery reports (returned to the user via email). • Appends the email address of the sender to the end of the message truncating the message if required for non-anonymous messages • Sets the ‘from’ address of the SMS message to a designated email address where the message is sent from an account with only outbound SMS capability	Y
3	User organisations must be able to administer gateway services for their users to: • Restrict or permit access for individual users. • Set and maintain quotas (fragment size, per message/per day recipient limits). • Report utilisation by account within their organisation	Y
Fax Gateway		
4	The Fax Gateway must provide an outbound email to fax service containing the following functionality: • Validates Fax content and size before sending.	Y

	• Encrypts user data in transit to the entry point to the telephone network. • Provides non-delivery and delivery reports (returned to the user via email). • Disallow specific numbers and number ranges specified centrally once and by the user organisation. • Add a national cover page detailing the sender, subject, recipient and number of pages to each fax	
5	The Fax Gateway may provide an inbound fax to email service.	
6	The fax Gateway must support multiple attachments of the following types: • Microsoft Office Word, Excel, and PowerPoint 2007, 2010, 2013 and onwards formats. • Adobe PDF format. • Open document formats. • RTF • A range of picture formats including but not limited to JPG, GIF, TIFF, PNG and BMP.	Y
7	The Fax Gateway must allow each user to send a Fax to multiple recipients. These can be entered manually or selected from a personal address book or from the Directory.	Y
8	Not used. •	Y
9	User organisations should be able to administer gateway services for their users to: • Restrict or permit access for individual users. • Set and maintain quotas (maximum pages and per message/per day recipient limits). • Monitor individual faxes sent.	
General		
10	The SMS and Fax services must support static and dynamic distribution lists for SMS and fax recipients.	Y
11	The SMS and Fax services should provide the ability to send anonymous messages on a per user basis, with organisational control.	
12	The SMS and Fax services must provide the ability to block delivery to SMS numbers and Fax numbers e.g. premium rate numbers. Currently this is platform wide but if Organisations locally pay for SMS for example then this should support per organisation/per account changes where an Organisation may wish to pay for sending SMS messages to international numbers. Currently the following UK dialling prefixes are permitted: 01, 02, 03, 055, 071-075, 077-079, 080, 084, 087 with 10 or 11 digit numbers only permitted.	Y
13	The SMS and Fax services must provide the ability to block access to features/functionality at a platform, organisation and user level e.g. adding new inbound SMS numbers.	Y
14	The service must utilise the following naming convention for outbound	Y

	messages: For SMS number@sms.nhs.net For Fax number@fax.nhs.net	
15	The service must provide delivery/non delivery reports which include as a minimum sender address, recipient address, sent time, delivery time, subject, SMS/Fax providers unique reference, email message ID. In the event of non-delivery the message should also include explanatory text to the reason e.g. blocked number or message too large. Non-Delivery reports should be configurable to be sent to another email address than the originator	Y
16	The NHSmail email disclaimer must be excluded from the message	Y
17	The service must support a configurable expiry time for both SMS and Fax messages.	Y
Search		
18	The Portal for the Fax and SMS services must provide a powerful search and browse function, with the ability to search (and filter search results) by organisation, account, fragments/pages and other criteria.	Y

2.8 Email Router

2.8.1 Outcome

The service will be used to integrate distinctly separate email services, for example a locally run NHS or private sector supplier with their own email service. As long as the email service meets the same set of minimum security standards as the NHSmail service it will be issued with local @nhs.net addresses for its users and added to the directory. The email router will ensure that the emails arrive at the right place.

Services issued with an @nhs.net address will only be able to send securely to other @nhs.net addresses i.e. the service will not act as a relay for them to other secure domains unless the local service is fully accredited to the determined security level.

2.8.2 Current Situation

Currently there is no provision for accrediting and integrating locally managed email systems into NHSmail other than the secure government domains so there is no need for an email router.

2.8.3 Requirements

#	Requirement	Essential
1	The Email Router must process all emails for the @nhs.net domain and sub-domains	Y
2	When an email is sent to the nhs.net domain or sub-domains, the Email Router must receive the email, determine the correct destination for it from the Directory Service and forward it through to the correct service Supplier.	Y
3	The Email Router must maintain the security and integrity of the email throughout.	Y

4	The Email Router must not store emails beyond the period necessary to forward them on.	Y
5	When processing a request for a new email address, the email router must be responsible for ensuring that the address has not already allocated to a user by another supplier.	Y
6	The email router must have robust technical and procedural controls in place for updating/managing approved local email systems to avoid potentially insecurely routing sensitive email	Y

2.9 nhs.uk Email Gateway

2.9.1 Outcome

There is a central email gateway for nhs.uk email services operating on PSN.

2.9.2 Current Situation

A number of NHS organisation run their own local nhs.uk email service. These systems operate at no security level or accreditation and in some cases utilise internet email routing. For those services operating on the N3 network the central nhs.uk email gateway (referred to in the NHS as the Relay Service) checks all messages sent and received for spam and viruses. In February 2013 the service checked email for just over 1,800 email systems supporting just over 3,000 nhs.uk email domains. The service utilises its own internet gateway to send/receive email for non nhs.uk email addresses and the N3 network to send/receive email for nhs.uk email addresses.

The nhs.uk email gateway does not process any sensitive data as if any sensitive data needs to be exchanged it is the responsibility of the sender to encrypt the content prior to transmission.

The service relies completely on the N3 DNS service for routing email and maintaining an internal (N3) and internet facing set of mail routing records. It is currently assumed that this service will continue to be provided in the future.

The service does not need to provide any service for those Organisations running their nhs.uk service over the Internet.

It should be noted that many of the common requirements do not apply to the nhs.uk email gateway. The decision to replace this service is currently under review and once confirmed the applicable commodity elements for this service will be explicitly listed.

2.9.3 Requirements

#	Requirement	Essential
1	The nhs.uk email gateway must accept email from any N3/PSN connected nhs.uk email service verified by reverse DNS lookup and relay it via the private DNS service for nhs.uk email addresses and the internet DNS service for all other email. Email for the Internet will be routed via the service providers own Internet connection. Where a connection is authenticated with a username/password the service should disregard the credentials and accept the connection anyway.	Y
2	The nhs.uk email gateway will receive email destined for nhs.uk email addresses via its own internet connection and relay it via the private DNS service.	Y
3	The nhs.uk email gateway must provide non-delivery reports for email messages which are unable to be delivered by it.	Y
4	The nhs.uk email gateway must contain functionality to support secure MIME standards.	Y

Email Hygiene		
5	The nhs.uk email gateway must provide industry leading anti-virus and anti-spam filtering. In addition to commodity virus/spam detection the service should also support attachment blocking.	Y
Data Retention and Compliance		
9	The service should only retain data necessary to support message delivery tracking in the event of delivery issues for up to 3 days as local nhs.uk email systems retain any data needed for compliance purposes.	Y
Reporting		
10	The service should provide a capability to support local billing should it be introduced in the future providing monthly volume reports by domain.	

3 Common Components

All of the following components are common to each of the individual components in Section 2 above. The table below shows how they apply

3.1 Access

3.1.1 Outcome

To offer a full service regardless of whether users are accessing NHSmail services using a desktop client or web browser. For some organisations, a web browser will be the only way for users to access NHSmail services.

3.1.2 Current Situation

Accessing NHSmail through a browser currently only provides part of the full functionality offered when using a desktop client such as Microsoft Outlook. When accessing via browsers other than Internet Explorer, the functionality of the portal is currently restricted, due to a Microsoft Exchange 2007 limitation.

The following browsers were used in December 2012:

Browser	Percentage
Internet Explorer 9	4.2%
Internet Explorer 8	17%
Internet Explorer 7	53%
Internet Explorer 6	8%
Google Chrome	5.9%
Safari	5%
Unknown	4.3%
Firefox	2.10%
Android browser	0.30%

As shown above, Internet Explorer accounts for 82.2%. Almost all corporate NHS desktops use Internet Explorer.

3.1.3 Requirements

#	Requirement	Essential
1	The services must be accessible via the following methods: • Desktop clients including but not limited to Microsoft Outlook and Mozilla Thunderbird • Web clients including but not limited to Internet Explorer, Firefox, Google Chrome and Safari • Mobile device clients (smartphones, tablets, etc) • Applications (e.g. Spine)	Y

	The intention is not that the services must support every possible version of desktop clients, web clients or mobile devices available. They should instead support a decent range of the current and previous two versions of the desktop clients, web clients or mobile devices most commonly used.	
2	Access to content must be based on the integrity of the device connecting. Fully secure endpoints will be granted full service access with the ability to locally download and cache content. In the case of email this could be holding an offline copy of the mailbox. Where an endpoint has no assured protection of data in use or at rest only browser access with no locally cached content should be available.	Y
3	All client server communication will be encrypted	Y
4	Browser access must be compliant with the appropriate web standards including HTML 5 support.	Y
5	Browser access must be compliant with the appropriate accessibility standards and guidelines including but not limited to WCAG 2.0 AA compliance.	Y
6	Browser access may provide all of the functionality of desktop clients.	
7	Browser access must prevent documents being downloaded to unsecure devices, such as public access computers.	Y
8	Browser access must comply with NHS branding requirements.	

3.2 Administration

3.2.1 Outcome

Health and care organisations can easily administer their organisation and users on the services. They can also administer “child” organisations, e.g. a CCG administering its GP practices.

Individual organisation identity and administration is important in the NHS as is the ability to manage other organisations with inherited permissions for ‘child’ organisations and the ability to add in ‘sibling’ organisations.

3.2.2 Current Situation

A range of administrator tools is provided for the current NHSmail solution that facilitates account management, distribution list and non-person account management.

3.2.3 Requirements

#	Requirement	Essential
Administration		
1	The service must allow full lifecycle administration including creation, deletion and suspension of accounts.	Y
2	The service must allow for multiple administrators.	Y
3	Administrators in organisations must be able to remove user accounts, including detecting and removing duplicate accounts.	Y
4	The supplier should consider providing administrators with the ability to restore expired accounts, and for account owners to be able to do it themselves through a safe method such as shared pre-registered secrets.	
5	The supplier should retain removed and expired accounts for a period to be agreed, and this period must be configurable in the event of any agreed policy changes.	
6	The supplier must provide the ability to undertake all necessary administrative tasks through an authenticated role based web user interface or programmatic interface. It should be possible to undertake actions on items both individually and in bulk. Administrators may manage more than one related and non-related organisation.	Y
7	The supplier must provide RBAC (Role-Based Access Control) and LBAC (Location-Based Access Control) administration. Availability and scope of administrator functions should be controllable by role and location through all the interfaces.	Y
8	The service must support platform, organisation and user level rate limiting controls based on number of messages sent and/or received per day, the message size, the number of recipients (vendor to detail how they count recipients on a DL) or in the case of SMS/Fax fragments/pages.	Y
9	Email addresses of deleted accounts should only be made available for re-use after an agreed period of time.	Y
10	When transferring an account to another organisation some attributes must be transferred (e.g. name, email address for life and quota), some	Y

	attributes removed (e.g. local email address and administration permissions) and some attributes updated/replaced (e.g. organisation details local email address). The account lifecycle management system must be configurable to support attribute transferrable, removal and updating/replacing.	

3.3 Onboarding and Offboarding

3.3.1 Outcome

The need for an organisation to move an existing NHSmail solution to the next NHSmail supplier with minimum effort and disruption is also important and should take place with no unreported data loss. Users will expect that their emails, contacts, tasks, documents and calendar appointments will all move with them, and it will be a very significant issue and cost to the business if any of these are lost, or the business is unable to use email during the migration.

The Customer is looking for tools to enable the easy migration of email accounts. This includes the migration from the existing service.

Ancillary data such as permissions, passwords and audit information all needs consideration to support a great transition experience.

The timescale expectation for transition is currently 3 month planning and 6-9 months to complete the transition.

3.3.2 Current Situation

NHSmail provides tools to take on organisations on an individual basis. There are no tools in place for migration from the existing platform to the new. This will be an important part of the NHSmail 2 project.

3.3.3 Requirements

#	Requirement	Essential
1	For each component suppliers must provide the ability for an organisation to move all its specified accounts and associated data (e.g. emails, contacts, tasks, calendars, distribution lists, ancillary data, email address or cloud storage content) across NHSmail 2 suppliers with minimal disruption and no unexpected data loss.	Y
2	Each supplier must allow migration to occur with minimal impact on organisations, and must require minimal effort from users and their administrators.	Y
3	Each supplier must provide the ability for an organisation to move all its specified accounts and associated data (e.g. emails, contacts, tasks, calendars, distribution lists, ancillary data, email addresses, directory content from the existing NHSmail service or in the case of local migration their local email service to the supplier’s NHSmail 2 service with minimal disruption and no unexpected data loss.	Y
4	For staff leaving or joining an organisation, and for organisational restructuring, the supplier must provide functionality to release items to other organisations, or to mark items for removal.	

3.4 Information Security

3.4.1 Outcome

The information held within the services is held securely in accordance with industry and public sector standards. The security mechanisms do not inhibit legitimate uses for the information. The services are accredited to an appropriate Business Impact Level (BIL or IL) with the G-Cloud. There is a suitable accreditation framework for sensitive personal data in health and care.

3.4.2 Current Situation

The NHS has not traditionally used central government security accreditation but does recognise the considerable expertise contained within it. This is partly historical and partly because the Business Impact Level system does not elegantly handle the working environment and practices of the NHS. The NHS is working with central government to address these concerns as part of a wider review of security accreditation.

The current NHSmail services have been given a departmental accreditation of Business Impact Level (IL) 3 with a single waiver, allowing access from uncontrolled end points over the internet. The expectation is that this caveat will continue for the new service but with some additional risk mitigation. The main drive for the IL3 requirement is that the service contains significant volumes of sensitive personal/ medical data.

3.4.3 Requirements

#	Requirement	Essential
1	Each Supplier must at all times maintain a secure service.	Y
2	The service must be robustly accredited to the security levels defined.	Y
3	Suppliers should implement one of the following for account access when not using an official health and care network (such as the NHS network): • A recognised form of two-factor authentication. • A mechanism that augments the strength of username and password.	
4	Each supplier must provide the ability for users to safely perform self-service password resets from any network utilising one of the methods described in requirement 3.	Y
5	The service should provide the ability for the login to be part of another single sign-on solution, such as that being considered for the Spine, or integration with an organisations existing solution, e.g. using SAML 2.0 integration.	
6	Each supplier must provide organisation administrators with tools to set per user and per client type access to individual components to support their local information governance policies. Additionally organisations would like to have a capability to identify personally owned equipment so that they can manage the risk and if need be block access to personally owned devices that do not comply with local information governance policies.	Y
7	Each Supplier must maintain an Information Security Management System (ISMS) that conforms to ISO/IEC 27001 Information Security Management	Y

	Systems and BS ISO/IEC 27002: 2005 IT. Security Techniques. Code of practice for information security management. Conformance may be evidenced by a certification from a body accredited by an appropriate National Authority. In the UK this is the United Kingdom Accreditation Service (UKAS).	
8	Each Supplier must maintain a security policy which sets out the security measures to be implemented and maintained in accordance with ISO/IEC 27001, BS ISO/IEC 27002 and the Information Security Management System. The security policy will be reviewed and updated in a timely fashion and will be reviewed on an annual basis.	Y
9	Each Supplier must conduct tests of the security policy in accordance with the provisions of the Suppliers Security Policy relating to security testing. The tests must be independently audited by either an accredited 3rd party or representatives of the Customer.	Y
10	Either party must notify the other immediately 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.	Y
11	Each Supplier should comply with the open standards policy: http://www.cabinetoffice.gov.uk/openstandards	
12	Suppliers should comply with the provisions of ISB 0129 Patient Safety Risk Management System - Manufacture of Health Software.	
13	Each supplier will provide protection against malicious content for their services such as virus checking when onboarding data.	Y

3.4.4 Security Levels

The service has been independently risk assessed against the HMG security policy framework information risk management standards (IS1 and IS1). This has resulted in a recommended impact level for each area of the service detailed below.

.

Service Element	BIL for Confidentiality	BIL for Integrity	BIL for Availability
Secure Email Secure Email Gateway Remote Storage Instant Messaging & Collaboration White Pages & Directory	BIL4	BIL4	BIL4
Client Access Mobile Access Web Access Mobile Device Management Fax Email Gateway Email Router	BIL3	BIL3	BIL4
SMS nhs.uk Email Gateway	BIL0	BIL2	BIL2

It should be noted that the there is no intention to purchase a pan government accredited IL3 or IL4 service, this assessment purely highlights the impact levels that would be required if these services were to be operated under the HMG Security Policy Framework

End point compliance is outside of the accreditation scope of the NHSmail 2 Programme. It is the responsibility of the connecting organisation to ensure they maintain end point compliance through both local/national policies/controls complimented by the tools provided by the NHSmail 2 service. National policies include for example the NHS Information Governance Statement of Compliance which sets out the requirements end points must adhere to when connecting to the NHS Network such as at rest encryption, patching and anti-virus software. These standards are outside of the control of the NHSmail Programme.

3.4.5 Departmental Accreditation

Due to the unique way that the NHS operates and provides services there are a number of controls that are not practical to operate such as allowing the service to be used by non UK staff and from end points that operate in public spaces such as a hospital or GP practice. The NHS recognises the importance of security and the value of the HMG framework and will use the elements of the HMG framework for the relevant impact levels of each service that can be applied to the NHS ways of working.

For any service identified as requiring to operate at IL2 or higher the intention is to consider IL2 pan government accredited services that meet the requirements and departmentally accredit against the NHS relevant IL3 and/or IL4 control sets.

3.5 Service Management

3.5.1 Outcome

The services are managed across multiple commodity suppliers. Each supplier shall provide industry standard levels of service management to its customers. Each supplier will provide a Service Desk which is accessible to the local service desk of all consuming Health and Care organisations. Where there is a direct connection between services e.g. Core email and Directory a relationship should exist between suppliers to enable appropriate incident handoffs.

The Customer's Service Management Team will manage supplier's performance through appropriate Service Levels and will facilitate cross supplier working where service interdependencies exist.

Current Situation

As the current service is provided by a single supplier, they manage the entire service from a single Service Management organisation. This organisation is ISO20000 certified and interfaces with the Customer's Service Management across all ITIL disciplines. The service desk provides a single point of contact and currently services circa 9000 contacts per month.

Requirements

The requirements are divided into sections for SMS and fax suppliers and other suppliers. Please see the relevant sections below.

3.5.2 Requirements (Not Applicable to Fax and SMS Suppliers)

#	Requirement	Essential
Service Management		
1	Each provider shall have an IT service management framework using processes that are based on ITIL or equivalent best practice guidance. Demonstrating the capability of the organisation by achieving certification to the ISO/IEC 20000 standard or an equivalent standard is desirable.	Y
2	Each provider shall interface appropriately, where required, with the Customer's ITIL aligned Service Management processes, ensuring appropriate peer contacts, process interfaces and deliverables are made available to support those processes and the integration of services that make up NHSmail.	Y
3	Each provider should provide a feed of live service monitoring to Customer's Service Management	
4	Each provider shall implement a comprehensive Performance Monitoring System to monitor and measure the performance of services being delivered and performance against agreed Service Levels and Key Performance Indicators	Y
5	Each provider shall permit the Customer to publish service performance information via media which may be visible in the public domain	Y
6	Each provider should utilise an ITIL based Service Management toolset	Y
7	Each provider shall work collaboratively with the Customer and other Service Providers, when reasonably requested, in circumstances such as when an integration issue has occurred and the root cause is unknown. Such activities will be led by the Customer's Service Management.	Y
8	Each provider shall apply a set of Incident and Problem Severity classifications. It is expected that these classifications are based on the impact and the urgency of the Incident / Problem. As an example, please see the example severity guidelines which many of the national suppliers adhere to currently.	Y
9	The Supplier must allocate each Incident Record with a unique reference number when the Incident is Logged on the Supplier's Incident Management Tool. This reference number must be provided to the party logging the Incident.	Y
10	The Supplier shall provide an audit trail of any incident actions and resolution activity upon request for a period of 12 months.	Y
11	Each Supplier shall provide diagnostic scripts, tools, knowledge articles, and training materials to enable customer's service desks to triage incidents, support local resolution, and capture the information necessary to resolve incidents. These must be subject to continual improvement.	Y
12	Each Supplier will own and actively manage all Incidents, Problems and Service Requests logged through its Service Desk or raised proactively until an appropriate resolution is effected and confirmed by the end users affected	Y
13	Each Supplier should allow authorised users access to their incident management tool to review the status and progress of their Incidents and Service Requests. This may be via a self-service web portal or similar.	

14	Upon identification that the activity required to resolve the Problem resides outside of the Supplier's boundary of responsibility the Supplier should immediately refer the problem to the appropriate party where one exists. The Supplier should retain an open problem record until the accepting party confirms resolution of the Problem. Any dispute between the parties shall be referred to the Customer.	
15	Each Supplier should make available a copy of its Problem Tracker on a regular basis to reflect updates to the status of Problems	
16	Each provider should present notification of changes to the Customers Service Management Team in sufficient time to allow integrated suppliers to impact assess and test the change appropriately. For normal changes, the expectation would be a minimum of one weeks' notice.	
17	When planning a Release, each provider should ensure that the timing of the release is notified to the Customer's Service Management team, with the opportunity to provide feedback and objection, at least 3 months before the planned release date.	
18	It is the responsibility of the provider to ensure sufficient capacity to meet the future needs of health and care organisations. All information utilised in the management of capacity should be made available for review by the Customer.	
19	Each provider shall agree a set of appropriate Service Levels which shall be monitored, measured and reported against to the Customer at least on a monthly basis. These Service Levels must include availability at a minimum of 99.9% and the following desirable service levels: • Response Times of user interactions with the service e.g. login, view an email • Email Delivery times within the NHSmail service • Incident Fix Times • Service Desk Performance • As an indication, please see the Service Levels in place on the current service, detailed in Appendix 1	Y
20	Each provider should host a regular Service review to review the previous periods service performance and agree performance against Service Level Agreements	
21	Each provider should comply with the provisions of ISO/IEC 22313 – Societal security -- Business continuity management systems	
22	Each provider shall deliver a Business Continuity and Disaster Recovery solution which allows for the agreed service levels to be maintained at all times, even in the event of a catastrophic event	Y
23	Each Supplier should deliver a Business Continuity and Disaster Recovery Plan to the Customer for review on an Annual basis – or following any significant change to the services. Any material issues with the plan must be addressed by the supplier	Y
24	Each provider should prove their Business Continuity/Disaster Recovery solutions with an annual test which will be independently witnessed and assured	

25	Each provider should demonstrate that continuous improvements are made to the service delivered based on both proactive activities and user feedback	
Service Desk		
26	The provider Service Desk must accept Incidents and Service Requests by at least the following means: • Telephone. • Email. • Web Portal.	Y
27	The provider Service Desk Telephone number should be via a single, published number which is either free or standard rate charged to landlines	
28	Each provider should publish an appropriate Escalation process	
29	Each provider should publish an appropriate Complaints process	
30	Upon identification that the activity required to resolve the Incident or Service Request resides with another NHSmail Service Provider, the provider should immediately log an Incident or Service Request with the appropriate Service Provider. The Supplier should retain an open incident record until the accepting party confirms acceptance of the incident. Any dispute between the parties shall be referred to the Customer.	
31	The Provider's Service Desk shall at all times reasonably co-operate with the Health and Care Service Desks and the Customer in the investigation and resolution of Incidents associated with the Contractor's Services and with services provided by Related Service Providers.	Y
32	Each provider shall provide a mechanism for communicating the current status of the services out to the user community. It is acceptable for this communication to be self-service; however, a 'push' mechanism would be desirable. The use of social media is an acceptable mechanism. In the case of severity 1 and severity 2 Incidents (or equivalent for the two highest impact/urgency incident categories), the updates on the status of the Incident should be at intervals of no greater than 30 minutes for Severity 1 (or equivalent) and 60 minutes for severity 2 (or equivalent), or as otherwise requested by the Customer.	Y
33	Each Supplier's Service Desk should provide the originator of the Incident or Service Request with regular communications on the status and progress of the Incident or Service Request	

3.5.3 Requirements (For Fax and SMS Suppliers Only)

#	Requirement	Essential
Service Management		
1	Each provider must have an IT service management framework appropriate for the management of Fax \ SMS service. The processes should be based on ITIL or equivalent industry recognised best practice guidance. Demonstrating the capability of the organisation by achieving certification to the ISO/IEC 20000 standard or an equivalent standard is desirable.	Y
2	Each provider must communicate details of any service impacting change out to consuming and funding organisations with a minimum of 7 days' notice for planned changes and as much notice as is reasonably available for	Y

	emergency changes. It is acceptable for this communication to be self-service; however, a 'push' mechanism would be desirable.	
3	Each provider must provide a mechanism for communicating the current status of the services out to consuming and funding organisations. It is acceptable for this communication to be self-service; however, a 'push' mechanism would be desirable. The use of social media is an acceptable mechanism.	Y
4	Each provider must implement a Performance Monitoring System to monitor and measure the performance of services being delivered and performance against agreed Service Levels and Key Performance Indicators.	Y
5	Each provider must agree an appropriate set of Service Levels for the services provided. Availability of the Services, Delivery Times of SMS/ Fax within the boundary of their responsibility and Fix Times for all Incidents, broke down by Severity would be appropriate. For details of the current ALS's please see Appendix I.	Y
6	Performance against SLA must be published via a mechanism accessible to all consuming and funding organisations.	Y
7	Each provider must work collaboratively with the Customer and other Service Providers, when reasonably requested, in circumstances such as when an integration issue has occurred and the root cause is unknown.	Y
8	Each provider will make available a mechanism for users to log Incidents and Service Requests related to the services provided. A telephone channel would be desirable.	Y
9	Each provider must publish a complaints process visible to all consuming and funding organisations	Y
10	Each provider must publish an escalation process visible to all consuming and funding organisations	Y
11	Each provider must implement appropriate capacity management processes to ensure that there is sufficient on-going capacity to meet the future demand of consuming organisations	Y
12	Each provider must host a regular Service review with Customer to review the previous periods service performance and agree performance against Service Level Agreements	Y
13	Each provider should implement appropriate Disaster Recovery provisions to ensure the continuity of the services, in line with the agreed SLA's, in the event of a disaster	
14	Each provider should test the Disaster Recovery provision annually. A copy of the test report being made available to consuming and funding organisations is desirable.	

3.6 Customer Service

3.6.1 Outcome

The services must provide excellent customer service to health and care organisations, their users and the Customer. This must be measured regularly and acted upon. If a service Supplier does not maintain excellent customer service then ultimately they will be replaced.

3.6.2 Current Situation

The Customer currently maintains long term (10 year) relationships with its suppliers. Whilst this results in a robust service and a good understanding of each other needs it does not lend itself to innovation and can result in too frequent consultation of the contract. There is clearly a balance to be struck with trade-offs.

3.6.3 Requirements

#	Requirement	Essential
User Surveys and Feedback		
1	Each Supplier should implement mechanisms to gather feedback from users on their service and report on them. The report must be published to all users of the service.	
2	Each Supplier should respond to feedback in order to improve the service as part of a programme of continuous improvement.	
Training		
4	The service must provide appropriate training for its users. This must include all aspects of the service.	Y
Purchase to Pay		
5	Each Supplier must support purchasing of services from: • The Customer • Health and care organisations. This must include individual billing for services.	Y
Quality Management		
6	Each provider should conform to ISO 9001. This must be demonstrated with a certificate from a body accredited by an appropriate National Authority which in the UK is the United Kingdom Accreditation Service (UKAS).	
Green IT		
7	Each provider should ensure that the data centres providing the service abide by the EU Data Centre Code of Conduct.	
8	Each provider should demonstrate that they have Green IT policies in place and that they are adhered to.	

3.7 Data Retention and Compliance

3.7.1 Outcome

Data is managed in accordance with legal, policy and good practice. This covers the Data Protection Act and the Freedom of Information Act.

3.7.2 Current Situation

The NHSmail service provides a set of tools for administrators to manage data retention and compliance.

3.7.3 Requirements

#	Requirement	Essential
1	Self-service deleted items recovery (minimum of 30 days)	Y
2	The service should support a self-service mailbox recovery capability.	
3	Copies of all email sent and received (minimum of 90 days)	Y
4	Copies of the message summary (in essence mail headers) of all emails sent and received (minimum of 2 years)	Y
5	System Audit logs (minimum of 6 months)	Y
6	Data to be captured in the Audit Trails will be sufficient to monitor whether 'Services' access controls are operating as intended.	Y
7	Automated audit analysis tools must be provided to assist auditors in the detection and prevention of system misuse.	Y
8	Data to be captured in the Audit Trails must be sufficient to identify who did what activity. For the purpose of email, calendar, contacts and tasks individual transaction item logging is not required just the login/logout events due to the volume of per message activities. However other parts of the service should retain sufficient detail to for example identify the specific administrator that used the administration tools to rename an account and capture the values changed. Where delegation is used to perform an activity the audit log should identify the delegate and who the delegate is performing the activity on behalf of.	Y
9	Retained data must be captured and made available robustly enough to support evidential use such as an internal disciplinary hearing or through the criminal justice system. It should also be recognised that there may be occasions that require very rapid (near real time) access to audit data.	Y
10	There should be a self-service ability to access audit data by authorised staff. Access should be limited to the scope of the service component the authorised user has access to e.g. email or Cloud Drive and any searches or return of data logged.	
11	The majority of audit requests relate to message tracing and a rich interface to support this should be supplied. There should be controls to help prevent abuse of this capability.	
12	There should be an option to increase data retention on a per Organisation basis (locally funded)	

3.8 Reporting

3.8.1 Outcome

User organisations and the Customer have sufficient information to easily administer the service in a user-friendly manner.

3.8.2 Current Situation

The NHSmail service provides a limited set of tools for administrators.

3.8.3 Requirements

#	Requirement	Essential
1	The service must provide reports to allow individual user organisations and the Customer to administer the service.	Y
2	The individual components must allow organisation administrators to run regular reports of the usage statistics of the service components. The reports must include (but not be limited to): • Volume of items sent by the organisation for the component (e.g. emails, faxes, text messages, files uploaded). Some items may include additional relevant data such as the size of email, number of fax pages or SMS fragments • Volume of items received by the organisation for the component (e.g. emails, text messages, files downloaded) • Number of accounts in use by the organisation (split by personal and generic accounts). • Number of expired accounts in the organisation. • Details relevant to components (e.g. per user quota status, mobile device report, items held in remote storage etc.) • Other items of the report to be finalised and agreed with the Customer. The reports must be exportable in a variety of open formats.	Y

4 Appendix 1 - NHSmail Service Levels

The tables below detail the current NHSmail Service Levels and provide an indication of performance against those Service Levels over the last 6 months (July 12 – Dec 12). It should be noted that the performance is measured only within the current supplier's boundary of responsibility so would not take account of issues related to N3, local infrastructure, etc

Abbreviations – OSL = Operating Service Level, FL1 = Failure Level 1, FL2 = Failure Level 2

Availability – measured monthly

Overall Availability has been achieved every month with the exception of October. Average actual Availability is 99.97%

Component Systems	OSL	FL1	FL2
All component Systems	>= 99.90%	< 99.90%, >=98.00%	< 98.00%

Application Response Times – measured monthly

These measures have been achieved consistently month on month for the most part, with only 7 individual measures having been failed in the last 6 months.

Transaction Description	OSL	FL1
Complete logon to Service	90% within 5s	85% within 5s
	95% within 15s	90% within 15s
	99% within 20s	94% within 20s
	100% within 45s	100% within 60s
View Email Message	90% within 2s	85% within 2s
	95% within 5s	90% within 5s
	99% within 10s	94% within 10s
	100% within 20s	100% within 30s
Unlock & Reset Password	90% within 5s	85% within 5s
	95% within 10s	90% within 10s
	99% within 15s	94% within 15s
	100% within 30s	100% within 45s
Authenticate user	90% within 5s	85% within 5s
	95% within 10s	90% within 10s
	99% within 15s	94% within 15s
	100% within 30s	100% within 45s
User Search Directory	90% within 5s	85% within 5s
	95% within 10s	90% within 10s
	99% within 15s	94% within 15s

	100% within 30s	100% within 45s
Administrator Search Directory	90% within 5s	85% within 5s
	95% within 10s	90% within 10s
	99% within 15s	94% within 15s
	100% within 30s	100% within 45s
Set Mailbox Quota	90% within 5s	85% within 5s
	95% within 10s	90% within 10s
	99% within 15s	94% within 15s
	100% within 30s	100% within 45s
Update Personal Details	90% within 5s	85% within 5s
	95% within 10s	90% within 10s
	99% within 15s	94% within 15s
	100% within 30s	100% within 45s
Change Security Questions	90% within 5s	85% within 5s
	95% within 10s	90% within 10s
	99% within 15s	94% within 15s
	100% within 30s	100% within 45s

Email Delivery Times- measured both daily and monthly

These measures have been achieved consistently, with only 5 individual daily measures and 1 individual monthly measure having been failed in the last 6 months.

Delivery Type	OSL	FL1
Email Service Mailbox to Email Service Mailbox	90% within 1 minute	85% within 1 minute
	95% within 3 minutes	90% within 3 minutes
	99.8% within 30 minutes	94.8% within 30 minutes
Email Service Mailbox to Fax Gateway	90% within 5 minutes	85% within 5 minutes
	95% within 1 hour	90% within 1 hour
	99.8% within 2 hours	94.8% within 2 hours
Email Service Mailbox to Internet Gateway	90% within 1 minute	85% within 1 minute
	95% within 3 minutes	90% within 3 minutes
	99.8% within 30 minutes	94.8% within 30 minutes
Internet Gateway to Email Service Mailbox	90% within 1 minute	85% within 1 minute
	95% within 3 minutes	90% within 3 minutes
	99.8% within 30 minutes	94.8% within 30 minutes
Email Service Mailbox to External Gateway	90% within 1 minute	85% within 1 minute
	95% within 3 minutes	90% within 3 minutes
	99.8% within 30 minutes	94.8% within 30 minutes
External Gateway to Email Service Mailbox	90% within 1 minute	85% within 1 minute
	95% within 3 minutes	90% within 3 minutes
	99.8% within 30 minutes	94.8% within 30 minutes

Email Service Mailbox to SMS Gateway	90% within 1 minute	85% within 1 minute
	95% within 3 minutes	90% within 3 minutes
	99.8% within 30 minutes	94.8% within 30 minutes

Service Desk

These measures have been achieved consistently over the last 6 months.

		Standard Required Operating Service Level (OSL)
Call Answer Times		
1	Answered within 20 seconds	>=90%
2	Answered within 40 seconds	>=95%
3	Average Answer Time	<= 20s
Emails Responded to within (based on emails requiring a response)		
1	60 Minutes	>=90%
2	2 Hours	>=99%
Abandoned Calls*		
1	% of calls Abandoned	<5%
First Time Fix		
1	% of incidents resolved by the helpdesk without the need for onward internal referral	>65%

*Calls only classed as abandoned if they have been in the queue for greater than 5 seconds.

Incident Fix Times

These measures have been achieved consistently for the last 6 months.

	SLA Levels		
Measure	**OSL**	**FL1**	**FL2**
Severity 1	<2h	2-3h	>3h
Severity 2	<4h	4-6h	>6h
Severity 3	<8h	8-12h	>12h
Severity 4	<48h	48-72h	>72h
Severity 5	<144h	144-216h	>216h

There is also a mail relay service that provides email relay, antivirus and anti-spam for nhs.uk addresses and bulk email applications.