# UHS requirements for
# Electronic messaging solution

V 1.0 FINAL

# 1   Section 1 – Basic electronic messaging requirements

## 1.1   Functionality

| New No | Requirement |
|---|---|
| 1 | At a basic level the solution must support one off messages between two users and confirm receipt |
| 2 | When the message has been read by a user the solution must   show an indicator to show it has been read. |
| 3 | It must be possible to message a user based on a desktop client from a web client and vice versa |
| 4 | The solution should support messaging conversations between two or more people and show who has read it |
| 5 | The solution should have a feature when messages have been read they can be deleted, discarded, saved etc. so the user is able to sort through messages and operate the solution efficiently. |
| 6 | Access to the messaging solution must be available through the following entry points<br>• App installed by users on their own phone<br>• App installed by Trust on trust phones<br>• Access via browser on desktop PCS<br>Access to the messaging solution should also available through the following entry points in the EPR solution:<br>• Function point within Dr Worklist<br>• Within web app for Dr Worklist (UHS side in development) |
| 7 | The solution should allow the user to seamlessly switch between a mobile device, phone and desktop  to carry on a conversation |
| 8 | The mobile app and the desktop app must be in sync |
| 9 | How will the solution work if the user puts their device on silent mode? What features can be used to ensure that users are alerted to new messages? |
| 10 | The supplier should describe how the user will know that the messaging solution is operational and that messages they are sending are being processed/ received. The solution should include the ability to notify the user when the messaging solution |

| New No | Requirement |
|---|---|
| | is not "active" i.e. to use the mobile device notification system, so they are able to take alternative actions. |
| 11 | The supplier should have a solution to notify users that messages have not been received. Unlike bleeps – phone may not sound or vibrate depending on user settings. Wireless and or 3G/4G cannot be expected to work all the time. What functionality does the supplier provide to ensure messages are received and give sender assurance / notification |
| 12 | The Trust wireless network is not in all locations across the site and there are some "dead spot". How will the solution tell the user they are in a "dead spot" and the messaging solution is not able to send and receive messages? |
| 13 | The messaging solution should allow users to exchange images, video and audio media messages |
| 14 | Supplier should explain storage for media outlined above and outline any impact on storage for these types of media |
| 15 | The solution should have the ability for users to embed [web] links within conversations. |
| 16 | The solution should allow the Trust to send global messages to all devices registered/ connected to the messaging system. |
| 17 | The global message function should be restricted to certain users as defined by the Trust |
| 18 | The solution should allow users to be able to archive old messages |
| 19 | The solution must not allow users to be able to delete old messages except via the Admin function. Suppliers should explain how they provide this functionality and whether it would be possible to prevent certain messages being deleted by admin e.g. Patient related.  The delete function must have a full audit trail. |
| 20 | The solution should allow messages to be categorised i.e. personal, patient related. |
| 21 | It should be possible to provide functionality that replicates "bleep batons" whereby a bleep is held by a person to provide a service for a period of time and then passed to the next person on the rota.  It could be that a user has multiple IDs and when they sign onto the messaging solution with the ID for on call role they are holding a "virtual baton bleep" |
| 22 | If a user is BYOD, and they come into work and do not sign in to the application to assign the bleep to their phone, they will not get any messages. The solution SHOULD provide some sort of cascade alert if this happens |
| 23 | Is it possible to have an on call group that always has active members that sign in and sign out? Is it possible to have a feature whereby the last user cannot sign off and leave the group empty? The Trust is looking for some sort of failsafe solution to ensure that a message group that is used for on call and to replace a baton bleep is not left "unmanned" |
| 24 | Is it possible to recall a message? |

| New No | Requirement |
|---|---|
| 25 | Does the solution includes a notify or escalate function based on urgency category and escalation if not read within a defined time period? |
| 26 | When the user logs into the messaging solution, it should be possible for the Trust to display messages that are customisable |
| 27 | Avoidance of message overload. What features does the solution offer to avoid message overload for the end user. The supplier SHOULD describe how they have considered this within their solution design. |
| 28 | Is there a log on process for the app and how does it work? |

## 1.2 BYOD

| New no | Requirement |
|---|---|
| 1 | It is intended that the solution will be primarily delivered on a BYOD basis for all staff using it. Supplier must confirm they can deliver via BYOD. |
| 2 | How will the solution support different BYOD devices and the minimum and maximum spec of devices supported. |
| 3 | If staff do not want to use their own device (i.e. BYOD) the Trust may have to offer a device to some groups e.g. porters, housekeeping staff. |
| 5 | The trust intends to implement a MDM solution. What is the experience of working with an MDM with a group of BYOD users? |
| 6 | The solution for BYOD must ensure that user's number will not be displayed or disclosed to other users. Suppliers should explain how they would deliver this functionality (use 141?). |

## 1.3 Use of the messaging solution around staff shifts

| New No | Requirement |
|---|---|
| 1 | The solution should have functionality to allow the user to switch off the messaging. For example when out of trust Wi-Fi limits |

| New No | Requirement |
|---|---|
|  | it should be possible to halt messaging such as the end of a shift the user may not wish to pay for data use on 3G/4G. |
| 2 | The solution should include a mechanism for filtering which can be used by staff when they are on holiday, off sick, off shift, on secondment or not wanting to be involved in a group conversation. They should be able to filter messages at group level e.g. turn off individual clinical groups but still see global messages. |
| 3 | It should be possible to restart messaging at any time (e.g. at home, before start of shift) |
| 4 | Staff should be able to log into the solution from home. |
| 5 | When messaging is reactivated it should be possible to see history of what has happened since you switched off |
| 6 | It should be possible for the staff to access the messaging solution via a desktop browser client via internet at home if required |

## 1.4   Alerts

| New No | Requirement |
|---|---|
| 1 | The solution should allow users to subscribe to receiving alerts |
| 2 | The solution should be configurable to allow for cascade of alerts i.e. pass an alert to another person or to a group. |
| 3 | The solution should have rules that direct the right alerts to the right staff members to eliminate unnecessary alerts. |
| 4 | The solution should allow users to subscribe to receive multiple alerts under different roles |
| 5 | The solution should allow the filtering of alerts so that off-duty staff aren't bothered by updates that don't occur during their shift. |

## 1.5 Groups

| New No | Requirement |
|---|---|
| 1 | The solution must allow admin to create groups |
| 2 | Users should also be able to create their own groups and select other users from a directory to add to the group |
| 3 | A manager must be allowed to manage multiple groups |
| 4 | Suppliers  must state if there is any limit in terms of number of users in a group |
| 5 | The solution should provide group management functionality to assign a manager to a group and allow them to manage that group. |
| 6 | The solution should allow users to be assigned to multiple groups |
| 7 | The solution should contain functionality such that users can log in and assign themselves to a group (if permitted) |
| 8 | A user should be able to re-assign themselves to different groups |
| 9 | The solution should allow the admin function to send messages to targeted groups of staff |

## 1.6 Directory

| New No | Requirement |
|---|---|
| 1 | The solution should   provide access to a directory of Trust staff – the information should be obtained from the Trust AD |
| 2 | It should be possible for the user to use their own phone book and add personal contacts into a group. Suppliers to describe how this will work with the Trust AD. |
| 3 | The solution should have a link with the device contacts database on the user's device and allow the user to initiate a call should that Device be a mobile phone. |
| 4 | When the user leaves the organisation they should be able to retain the contacts they have saved to their own directory from the Trust AD (although they will no longer have access to the Trust AD). We expect this requirement to be fulfilled by integration with the MDM but suppliers should explain how the "sandboxing" will work. |

### 1.7  Administration

| New No | Requirement |
|--------|-------------|
| 1 | The solution MUST   be easy to administer but provide sophisticated administration functionality. Suppliers MUST   describe the functionality. |
| 2 | The solution SHOULD allow the Trust to display terms and conditions for usage and to force the user to accept these before using the solution. The terms and conditions for usage SHOULD be configurable by the Trust. |
| 3 | The solution SHOULD allow the Trust to re-display terms and conditions for usage to existing users for a defined time period e.g. every 3 months and / or after application updates. |
| 4 | The solution MUST have an Admin function that should allow admin at multiple levels. For example the Trust would want to Administrate centrally certain functionality such as the addition of new users but may wish to delegate functionality to certain staff or roles for example the addition of staff to a group. This is a key requirement and suppliers MUST explain how their solution delivers this functionality. |
| 5 | The solution SHOULD provide the ability to monitor the presence in each group and highlight group presence indicators such as new members and the last one to log out. There SHOULD be alerts for these types of events. |
| 6 | Staff SHOULD be able to connect themselves to the messaging solution using their AD credentials |
| 7 | The solution SHOULD provide visibility of those currently connected to the messenger solution. This SHOULD be via a dashboard type solution. |
| 8 | The supplier SHOULD describe which administration functionality they would recommend is undertaken by a centralised Trust service for the messaging solution. (Suppliers SHOULD note that there is work underway by the Informatics service to merge the IT service desk and trust switchboard service into one which could potentially undertake this function. This will be a 24/7 service) |
| 9 | SHOULD a user account be disabled, the contacts that the user has saved to their own directory should be retained but the solution SHOULD delete messages from The Device upon next connection SHOULD an attempt be made [to connect] however the solution SHOULD not remove the messages from the system. |
| 10 | There SHOULD be a simple process to connect locum/agency/ temporary staff out of hours. Suppliers to describe options for undertaking this and their experience in other organisations. |
| 11 | There SHOULD  be a simple admin function for managing new staff (starters) and existing staff (leavers) |
| 12 | For the management of locum/ temporary staff who work with the Trust, when they go away and then come back there |

| New No | Requirement |
|---|---|
| | SHOULD be a feature to de-activate and re-activate an account. When the account is re-activated the history SHOULD be available. |

## 1.8  Non Trust users

| New No | Requirement |
|---|---|
| 1 | There is potential for the solution to be used across the wider health economy These non-trust users could be other Trusts including other acute services, mental health, community and ambulance. We also want to consider GPs, social services etc. What implementation model would the supplier propose to achieve this aim? |
| 2 | Please explain how this would work with regards to the administration function (these users will not be in the Trust AD). |

## 2 Section 2 - interface with EPR

### 2.1 Basic functionality for EPR integration

| New No | Requirement |
|---|---|
| 1 | The Solution should support interfacing to an EPR. Suppliers should detail their experience in doing this and provide examples of functionality implemented at other sites. |
| 2 | Suppliers must provide a statement on interoperability outlining their approach and strategy |
| 3 | An API for use by the Trust should be provided so that other trust applications can be integrated with the messaging solution over time |
| 4 | The solution should allow HL7 queries of the EPR systems<br><br>Clarification note<br><br>The HL7 message should include a segment identifying the data source and this then needs to be clearly displayed within the EPR. This would be the same solution as Point of Care testing and will be necessary otherwise EMIS won't accept the perceived risk associated with the EPR displaying data from a third party system. |
| 5 | if interfacing is proposed via HL7 then suppliers should explain their strategy for migrating to FHIR |
| 6 | The solution should allow the Trust to place a "function point" in the UHSFT EPR application Dr Worklist to say "lets chat" against a patient and this would launch the messaging application. |
| 7 | The solution should support web page product (icon or jump point) – point out and chat – ensuring that the right patient / right conversation is referenced. |
| 8 | EPR integration should be based on token based authentication using SSO concept – suppliers should explain how they achieve this. |
| 9 | The solution should include a "dashboard" that summarises the number of messages, the interface status, tasks etc. |
| 10 | Suppliers SHOULD indicate their relationship with bots and their strategy for this type of development in order to support the type of integration indicated in this section. |

## 2.2    Patient identification

| New No | Requirement |
|---|---|
| 1 | The solution SHOULD   link to the Trust Patient Record for patient details (demographics) from the PMI, It is our preference that FHIR is used. |
| 2 | It SHOULD be possible to search for the patient and their location in the Trust PAS and or the Trust TIE from the messaging solution. |
| 3 | Suppliers SHOULD  describe how they would present a list of patients to the user within the messaging solution |
| 4 | The solution SHOULD link to the Trust Patient Record for ADT messages relating to the admission, discharge and transfer of a patient. This SHOULD  include  the current patient location |
| 5 | It SHOULD  be possible to be alerted to a patient move which is recorded as a transfer on the PAS and a message to be sent to users who have registered an interest in that patient (i.e. they are part of their care group) |
| 6 | The solution SHOULD be able to request demographics via patient search and direct patient or NHS number. This to be attached to a conversation. This SHOULD be via HL7 or FHIR. |
| 7 | The solution SHOULD be able to support merge messages and migration of conversations to the correct patient number where an error in identifying the patient has been made. |
| 8 | Message conversations may be related to patients who are not currently inpatients although their details will be on the PMI. Suppliers SHOULD describe how they will facilitate a PMI search to support these. |
| 9 | It SHOULD be possible to associate users and groups on the messaging solution with a patient so they receive messages and alerts relating to that patient. |
| 10 | It SHOULD be possible to undertake a global search of messages. For example find me conversations about patient x or named individual y or subject z. |

## 2.3    Patient related messages

| New No | Requirement |
|---|---|
| 1 | The solution SHOULD   have the functionality to link a conversation to a patient through interfacing and to file such |

| New No | Requirement |
|---|---|
| | conversation SHOULD that be appropriate, in the record |
| 2 | The solution SHOULD be able Push conversation on demand to a patient record via the Trust Integration Engine (TIE). Supplier SHOULD explain which formats they will support. The Trust's EDM solution has a print to EDM function that could be utilised by the supplier to push messages into the EDM – suppliers should comment on the feasibility of this as a solution. |
| 3 | Suppliers should explain the triggers they could use to identify the end of a conversation- e.g. discharge – lack of activity on a conversation over a given time period. |
| 4 | For complex patients with extended LOS there may be a very long message threads. Interim filing in the EPR SHOULD be undertaken so there is an awareness that a patient related message thread exists. Supplier should outline how they would approach this e.g. update at midnight, version control of message threads, replace with new etc |
| 5 | If it is decided the message does not get filed into the patient record as it is not relevant is there functionality to undertake this. Suppliers should explain how this could /would work. |
| 6 | The messaging solution should allow users (e.g. Consultants) to give advice and guidance to another user or to a group and it SHOULD be possible to remove or insert this from a conversation about a patient i.e. start another message thread or link in a message thread. |
| 7 | The solution should allow archiving of messages |
| 8 | The message archive should be searchable |

### 2.3.1   Task Management – integration with DWL

| New No | Requirement |
|---|---|
| 1 | It is expected that Tasks will be initiated via the DWL and then pushed into the message solution. Suppliers are invited to describe any task management functionality within their emessaging application that would integrate/ compliment / work alongside the Trust DWL solution. |
| 2 | It should be possible for Group leader to co-ordinate the work of a group and allocate tasks/requests via the message |

| New No | Requirement |
|---|---|
| | solution/ DWL to members of the group. |
| 3 | It should be possible to allocate a task using the solution to a person or a group |
| 4 | The group or group leader SHOULD to be able to see status of tasks and re-allocate if required. |
| 5 | The solution SHOULD provide functionality that helps with assignment of tasks. This means that messages are sent to the right person based on his or her role and device preferences. Suppliers SHOULD describe how they provide this. |
| 6 | The status of a task SHOULD   be visible to the requester and the receiver |
| 7 | The status of a task SHOULD be visible to all members of the group |

## 2.4   Order communications

Please note we have described the integration with order communications at three levels of functionality

### 2.4.1   Level 1 – basic messaging with order communications (EQUEST)

| New No | Requirement |
|---|---|
| 1 | It SHOULD be possible to alert a user that a result they are interested in for a patient has become available on the Equest Order communications system. |
| 2 | If a group has registered an interest in patient then the alert that a result is available on Equest SHOULD be available to the whole group. |
| 3 | It SHOULD be possible for an alert to a group to become a task for action and the group manager to assign it to a member of the group. |
| 4 | It SHOULD be possible for a user within a group to easily indicate to other group members that they have actioned that result following the alert i.e. have logged into Equest to view it and sign it off. |

### 2.4.2 Level 2 – receipt of results from order communications (EQUEST)

| New No | Requirement |
|---|---|
| 1 | It SHOULD be possible for a result to be sent from Equest to the messaging system. Suppliers to explain how they would achieve this. That result should be sent to a group and any user with a registered interest in that patient.<br><br>Clarification – Results are not just numeric. They comprise of reference ranges, units of measurement, high/low flags, test result, request item, specimen comments. They can also be dynamic, matrices or textual. UHS will need to decide whether it would be better to send the result itself or the specimen order ID in the form of a secure hyperlink which can then open up the result in a hosted application. |
| 2 | It SHOULD be possible from within the messaging solution to scan the QR code on the patient wristband and receive via a message the latest lab results for that patient. |
| 3 | The messaging solution SHOULD be able to send a message to the Equest solution to say the result has been opened and read with details of the user. |
| 4 | It SHOULD be possible for a result to be seen and signed off /acknowledged by a user and that sign off to be sent back to Equest. Suppliers to explain how they would achieve this. That result should be sent to a group or user with a registered interest in that patient and the sign off may come from a user or a user within a group. The group SHOULD be able to see that action has been taken. |
| 5 | The solution SHOULD have the ability to present results to the user and add a response to the acknowledgement that goes back to Equest e.g. a comment. |

### 2.4.3  Level 3 – requesting via the messaging solution

| New No | Requirement |
|--------|-------------|
| 1 | It SHOULD be possible to raise an order for a service or test from the messaging solution via Equest. This is a part of the requirement for future stage of implementation. Supplier to outline how they would approach this. This would include referrals to other services that are initiated in eQuest but the messaging solution is used to send them, receipt and acknowledge them and return a response. |

## 2.5  Interfacing with the acuity solution (IMDSoft Safetrack)

| New No | Requirement |
|--------|-------------|
| 1 | The Trust wishes to provide acuity scores from the IMDSoft Safetrack solution and would like to put an API on the front of the solution to connect to the messaging system. Suppliers SHOULD state if this is possible.<br>It is planned to broadcast as needed in DWL for ePAMS phase 2. |
| 2 | When MEWS scores for patients registered on the IMDSoft Safetrack solution go up this should trigger a message to a user or group on the messaging solution |
| 3 | It SHOULD be possible to message vital signs at a user defined time period from the IMDSoft solution into the messaging solution for certain patients. |
| 4 | The solution SHOULD have a link to the UHS IMDSoft Mobile observation solution "Safetrack" such that a conversation can be started from the patient screen. |
| 5 | If a MEWS was escalated – you need an accept button to accept the task and a further alert to someone else if the task is not done within a certain timeframe. This must also send a notification back to say task not done. It must close the loop and provide a failsafe system. |

### 2.6 Other EPR integration requirements

| New No | Requirement |
|---|---|
| 1 | The Trust may wish to enable SMS messaging from other EPR applications. Suppliers SHOULD describe how this would be delivered and supported |
| 2 | The Trust may wish to launch the messaging solution from other applications e.g. corporate solutions. Suppliers SHOULD describe the process for setting this up and any restrictions that may apply. |

## 3    Information Governance requirements

| New No | sub section | Requirement |
|---|---|---|
| 1 | Audit | There MUST   be an audit trail of message activity. Suppliers SHOULD detail the content and functionality of the audit trail. |
| 2 | Audit | Through the admin function it must be possible to identify if the message occurred inside (on the Trust network) or outside the trust (on 3G/4G) |
| 3 | Cookies | The supplier must confirm that within the solution no cookies or browser history is saved |
| 4 | DP | The solution MUST    fully comply with the Data Protection Act (1998) |
| 5 | Encryption | Supplier MUST   outline their strategy for encryption. (Drafting note - A decision will need to be made on the level of encryption required. This could be end-to-end with only the recipients having data in the clear i.e. readable. The Trust needs to consider however whether it requires access to data at rest.) |
| 6 | Encryption | The security model MUST use data encryption SSL |
| 7 | GDPR | The solution MUST comply with General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) |

| New No | sub section | Requirement |
|---|---|---|
| 8 | FOI | How would the Trust query the solution in order to answer an FOI request? |
| 9 | Handling of mobile numbers | It would be an IG breach to disclose personal mobile numbers for staff. How will the solution keep these hidden even though we are using a BYOD approach? Will the solution add their mobile number into the UHS AD and how will they be stored? |
| 10 | IG | The solution MUST be capable of providing admissible digital evidence if required by an investigation or legal proceedings? |
| 11 | SAR | The solution Must allow the Trust to respond to Subject Access Requests (SARs). How will the supplier support this and what functionality is provided to support this? For example how would the SAR team search the messaging solution to find patient related messages? |
| 12 | SAR | Access to messages details through a SAR could create liability and professional issues for users of the system. What functionality has the supplier implemented or could provide to help manage this and reduce this risk e.g. messages around appropriate use. . |
| 13 | Screen lock out | The solution MUST have a time out which requires authentication to re-access. The timeout length SHOULD be configurable by the Trust. |
| 14 | Security | The solution MUST be a secure messaging solution hosted either on or off premise with no data leaving the European Union |
| 15 | Security | There MUST be a sandbox function – all conversations removed when the user leaves the organisation. |
| 16 | security | The solution MUST have functionality to prevent any unauthorised use of the messaging solution or any attempt to prevent its use e.g. a denial of service attack |
| 17 | Security testing | The solution MUST be tested for security. Suppliers MUST describe how they do this, how and when they re-test. |
| 18 | Biometric data | Is there any intention to use Biometric data for log on to the app? If so this would have a privacy impact that would need to be considered as we do not currently collect this data for our staff. |

# 4 Technical requirements

| New No | sub section | Requirement |
|---|---|---|
| 1 | Basic requirement | The app SHOULD works on both 3G/4G and Wi-Fi networks. |
| 2 | Basic requirement | The solution MUST be cloud based. If the supplier cannot provide a cloud based solution then they must detail the hardware requirements and confirm that the solution can be virtualised. |
| 3 | Basic requirement | The Solution MUST run in a desktop environment namely a MS Windows desktop with IE 11 but the supplier SHOULD also be browser agnostic. |
| 4 | Basic requirement | The Solution MUST run on the following mobile platforms as a minimum: iPhone; iPad Mini; iPad; Android devices (which ones to be stated by Supplier). |
| 5 | Download | The solution MUST be free to any member of staff including agency, contractors, locums and any temporary staff undertaking work for the Trust (as authorised by the Trust) |
| 6 | Download | The solution MUST be available for download on the internet (i.e. off-site from Trust premises) and from the Trust intranet |
| 7 | Active Directory | The solution SHOULD be integrated with the Trust's Active Directory. User accounts will link to the UHSFT MS Active Directory. |
| 8 | Active Directory | The supplier SHOULD outline any impact on the Trust AD as a consequence of the implementation of the messaging solution and any ongoing maintenance that might be required of the AD by the IT team |
| 9 | administration | There SHOULD be a technical management function support such as an overview of traffic and service status. |
| 10 | Back up | The Solution MUST be backed up, or there will be a means for the Authority to back it up. This will happen while the solution is operational. |
| 11 | Backward compability | Suppliers SHOULD describe how they approach backward compatibility for BYOD devices where there are known challenges e.g. Android devices |

| New No | sub section | Requirement |
|---|---|---|
| 12 | Conflicting apps | The solution SHOULD have a function to notify the user of any conflicts between other messaging software on their device. |
| 13 | Documentation | The supplier SHOULD provide a fully documented installation including all site specific configuration |
| 14 | Documentation | Technical documentation MUST be provided to allow UHSFT Informatics group to develop interfacings with the messaging solution from other Trust applications via an API |
| 15 | Functionality of user interface | The supplier SHOULD describe any differences in functionality between the mobile App solution and the desktop solution. UHS will need to know which components this applies to if not the whole Solution i.e. if there is a separate management function. |
| 16 | Hosted | If the supplier is proposing a Hosted service then fully details MUST be provided. The hosted service MUST be located in the UK. |
| 17 | IT standards | The solution MUST comply with the IT standards for UHSFT as detailed in section below |
| 18 | New releases and updates | The supplier SHOULD describe how they will implement new versions of the messaging solution and how the updates be applied |
| 19 | new releases and updates | Suppliers SHOULD describe their approach to version control and the impact of new versions on the users with BYOD who may not have the most up to date device, operating solution etc. How will they ensure that new versions of the software work with older or very new devices? How long will old versions of the messaging software continue to be supported after the new version has been implemented? |
| 20 | Resilience | The solution MUST be resilient and available 24/7, 365. Suppliers MUST describe their approach to resilience and how they assure high availability. |
| 21 | Resilience | The solution SHOULD have the ability to carry out solution maintenance with minimal or no downtime to the service users |
| 22 | MDM | Suppliers SHOULD state which MDM solution their solution has been implemented with. Which features within the MDM have been used to deliver greater security? |

| New No | sub section | Requirement |
|---|---|---|
| 23 | Integration | Suppliers SHOULD integrate with other Trust systems via the Trust Integration Engine (TIE). Suppliers SHOULD describe how they have integrated with other systems and provide examples of the message types they support, stating whether these are existing or planned messages. |

# 5 Other requirements

| New No | sub section | Requirement |
|---|---|---|
| 3 | Prime contractor | Supplier must identify any other suppliers working with them on providing the solution. Suppliers must confirmed they are prime contractor and would be accountable for all aspects of the solution, delivery and contract. |
| 6 | Termination – access to data | The Supplier MUST   agree that the data will be made available to The Authority in a format to be agreed at the time of Termination. |
| 7 | Topic forums | Suppliers SHOULD explain options for provision and whether their solution could be linked to topic forum. Suppliers to explain whether it would be possible to insert a link within a message to a topic discussion forum. |
| 8 | Other functionality | Suppliers are invited to describe other functionality within their solution which has not been identified in this specification of requirements but they believe would be of benefit to the Trust. Suppliers SHOULD explain why they think the functionality is beneficial and how they envisage it being used. |

# 6 Implementation requirements

| New No | Requirement |
|---|---|
| 1 | The basic functionality to be delivered on day 1 SHOULD allow UHSFT to replace all the current non-urgent bleeps with the messaging functionality. Suppliers SHOULD describe their go live process and how they would propose that this basic functionality is delivered. |
| 2 | Suppliers SHOULD describe their approach to implementation and how they would deliver the basic and more complex functionality described in their specification. It is expected the implementation plan would have a number of phases in order to deliver the full solution. |
| 3 | Suppliers SHOULD  outline the training approach they would propose for their solution and explain how this has been used in other implementations |
| 4 | Suppliers SHOULD  explain how they would support the "Culture change" that may be required to encourage staff to use this solution in place of the current unauthorised use of messaging |
| 5 | Suppliers SHOULD  explain the lessons learned from previous implementations of their solutions and how they will help the Trust to address these in this implementation |
| 6 | Suppliers SHOULD provide costs for pre-paid consultancy days as part of the initial contract which may be used at the discretion of the Trust for support or training of the products or services supplied and any interaction of those products and services with other Trust systems. |

# 7 Support requirements

| No | Requirement |
|---|---|
| 1 | There MUST   be a single contact for support |
| 2 | The solution SHOULD have 5 year / 24 hour / 365 days support. |
| 3 | Other options for support could be proposed if the supplier believes they are acceptable e.g. 8-8, M-F. Suppliers SHOULD state what support they provide for other customers. |

| No | Requirement |
|---|---|
| 4 | The solution SHOULD  have options for time-to-respond and time-to-fix support, e.g. 4 hour response or 6 hour repair |
| 5 | The supplier SHOULD provide multiple solutions for fault logging e.g. telephone, web based etc and ability for IT group to track progress on reported issues. |
| 6 | On-site supplier support SHOULD be available for software updates and patches if required. |
| 7 | Suppliers SHOULD outline the support they expect the Trust to provide through the admin function on a day to day basis. A general description of tasks SHOULD be provided. Any assumptions re level of skill, knowledge and experience for the admin function SHOULD be stated. |
| 8 | Supplier MUST have a fault management system. |

## 8   Optional requirements

| New No | sub section | Requirement |
|---|---|---|
| 1 | Alerts from clinical systems | The solution SHOULD provide the facility for Message alerts from key clinical systems to a defined group as configured by the Trust e.g. number of emergency admissions in a given period, expected emergency admissions for a specialty / service etc. |
| 2 | Alerts on events | The solution SHOULD provide the facility for standard messages to be developed and sent based on a logic, solution message, event, etc. Examples include discharge of an inpatient to send a message to housekeeping group to clean the bed space, admission of a patient with diabetes to alert the diabetes team, AKI status to alert appropriate team, etc. |
| 3 | Authentication | The intended strategy of the trust is to use Thumbprint authentication – suppliers SHOULD explain if this functionality is in their current product or part of their future development |
| 4 | BMS | The solution SHOULD provide messaging from fire alarms, security systems, building management systems.  It SHOULD enable alarms to be directed immediately to the appropriate member of staff. The Trust uses the Honeywell BMS solution. |

| New No | sub section | Requirement |
|---|---|---|
| 5 | External connectivity | The solution SHOULD have the ability to communicate securely with external agencies i.e. those not on The System. This will include the UHS e-mail solution and a secure link with NHS mail may be possible. |
| 6 | External connectivity | The Trust may wish messaging to be provided for staff working outside the organisation involved in the care of the patients – e.g. GPs, primary care, therapy staff, and nursing staff. Supplier SHOULD describe how this might be delivered. |
| 7 | Interface with BMS | The solution SHOULD interface with the Trust BMS via the Trust network and be able to undertake messaging such as automatically message the duty engineer. |
| 8 | Queries | The solution should be able to send a message to an application such as eprescribing to ask if x drug has been administered in last x hours? |
| 9 | Medical equipment | The solution SHOULD be able to receive messages and alerts from medical equipment |
| 10 | Message enabled devices | It SHOULD be possible to provide messaging from devices that are message enabled e.g. temperature monitoring on fridges |
| 11 | Nurse call | The solution SHOULD provide messaging from the nurse call system. It enables alarms to be directed immediately to the appropriate member of staff. |
| 12 | Patient ID | The solution SHOULD have the capability to scan barcodes on patient wrist bands to search for the patient identity details and record (current bar code formats are 2 D – QR, Linear, and GS1 – these may change in the future). This functionality SHOULD be provided by the device's in-built camera rather than any add-on bar code reader. |
| 14 | Speech recognition | Suppliers SHOULD explain if their solution provides speech recognition and if not whether this is in their road map for future development. |
| 15 | User location | It SHOULD be possible for a user to share their location via the messaging application as an optional setting |
| 16 | Video conferencing | It SHOULD be possible for the application to support video conferencing messaging for one to one and in groups. Suppliers to explain how this is provided. |
| 17 | See who is on call | A link to Rota Watch and or Health Roster would allow staff to see who is on call |

### 8.1 User feedback

| No | Comment from workshop participant |
|----|-----------------------------------|
| 1 | It would be great if photos can be taken and shared but not saved on the phone to get an opinion. For example here is the x-ray and here is a picture of what the injury looked like. |
| 4 | Would it be possible to link to Health Roster in order to find out who is on shift |
| 5 | if the messaging app was to be used for general discussion we would want to separate **general chit chat** from discussions around patients |
| 6 | There is a danger of mixing up different patients in message threads. There could be a long string of messages discussing several patents and it would not be clear which message relates to which patient. Then if you wanted to save that message string into the patient's electronic notes you might end up saving the wrong information with the wrong patient. Each message needs to have the patient identifier included so you can see which patient the discussion is about |
| 7 | If you are not available it would be good if you could set the messaging system to divert messages to the next available person e.g. your registrar |
| 8 | it would be useful if you could pre-programme in escalation such as if I do not respond within a certain amount of time to a message – send it to X |
| 9 | Will the implementation be customised for the specialty – different services work in different ways – what might work well for medicine may not work well for Obstetrics? Midwives work in a different way from Nurses. |
| 10 | Could you select what you wanted to fetch rather than being sent things |
| 11 | The solution should allow you to request and fetch rather than push information to you |
| 12 | If a diagnostic procedure such as an MRI got cancelled I would like to get a message to tell me |
| 13 | The export of information into the Electronic Patient Record solution should be a simple swipe action |
| 14 | You should be able to select a chunk / part of a message thread and send it as a record to the electronic patient record |
| 15 | it should be easy to search for a patient such as surname and first name |
| 16 | you must be able to drop out/ leave a conversations |
| 17 | it would be useful if you could set priorities to messages to ensure better time management – for example high priority messages come straight away but set delivery times for low priority messages so you can read them in a batch |
| 18 | you should be able to set a priority to a message where it either sits on a list or alerts you |
| 20 | The solution should have ticks to indicate the message/task has been read, accepted and done. There should be alerts if not read, accepted or done within a certain timescale. |

| No | Comment from workshop participant |
|---|---|
| 21 | if a task is sent by the messaging solution then a reasonable amount of time should be allowed to do it |
| 22 | Need to be able to re assign tasks when someone is overloaded. A more senior person should be able to reassign and set priorities |
| 23 | Can we link the messaging solution to the on call rota – would it be possible to ask who is on call and then place a call to them |
| 24 | Integration with systems, or is it interception of messaging through TIE? |
| 25 | Automate unexpected finding notification via report urgency transmitted to TIE (recognising specific referrer and their location.) |
| 26 | On hold events, notification to referrer and clinical lead that additional review required, event not progressing (ad hoc detail contained within status update messaging). Done based on HL7 messaging rather that via DM or bot? |
| 27 | Described as 'in the system', can it publish to other repositories based on image type/description?<br><br>Clarification - Regarding the point about whether images are stored on VNA or EDMS, in a nub the 'strategic decision' that was made a while ago was that system generated images such as those captured from an Endoscopy camera should be stored within the VNA.  These may be multiple images per patient or even video files and they are already linked to a patient/report at the time of generation which gives us some assurance around integrity of the records.<br><br>Images such as those taken by our medical photography team or by clinicians were going to be stored within the eDMS as there needed to be some manual intervention to ensure they were stored against the correct patient record.  The uploads will tend not to be real-time, instead they'll be done retrospectively after the event. |
| 28 | It saves with patient demographic; can it deal with auto registration on 'other' systems? (specifically, CRIS) or any plans to become a publisher for XDS VNA environments. |
| 29 | Radiology imaging...? integrated to PACS image store or photo of image? |
| 30 | Desktop version for admin teams. |
| 31 | In context launching into other systems (if on iPads). |

**IP Statement**



The Trust owns the intellectual property rights subsisting in all materials (including but not limited to any concepts, images, photographs, designs, drawings, texts, artwork, graphics, sound recordings, video and audio materials, logos, taglines, processes, know-how, business methods, programming codes, software and data) created for or developed by or on behalf of the Trust in the Global Digital Exemplar Programme (**"GDE Programme IPR"**). The Trust hereby permits you to use, copy, modify and/or develop of the GDE Programme IPR subject to compliance with the following conditions:

1. any use, copying, modification and/or development of the GDE Programme IPR is for non-commercial purposes;

2. you acknowledge that any and all intellectual property rights in any modifications, improvements, adaptations and/or derivative works created from the GDE Programme IPR by you (**"Derivative IPR"**) will vest in the Trust and upon the Trust's request you agree to execute documents and to do all acts necessary to ensure that legal title to the Derivative IPR vests in Trust and you waive, and agrees to procure the waiver of individuals engaged by you in the creation of Derivative IPR, any and all moral rights arising under the Copyright, Designs and Patents Act 1988 and so far as is legally possible, any broadly equivalent rights you may have in any territory of the world in the Derivative IPR;

3. you notify the Trust of any use, copying, development and/or modification of the GDE Programme IPR by notification to the following e-mail address: England.gdeblueprints@nhs.net;

4. you provide acknowledgements that the Trust owns the intellectual property rights in the GDE Programme IPR and Derivative IPR;

5. Upon the Trust's request, or the request of NHS England acting on behalf of the Trust, you provide (at the requestor's choice) physical or electronic copies of any Derivative IPR to the following e-mail address: England.gdeblueprints@nhs.net, or such other address as stated by the requestor.

Failure to comply with any of these terms will result in all rights and permissions ceasing automatically.