SUPPLEMENTARY MATERIAL

Moving from non-emergency bleeps and long-range pagers to a hospital-wide, EHR-integrated secure messaging system: an implementer report

Ari Ercole[1], Claire Tolliday[1], William Gelson[1], James H.F. Rudd[1], Ewen Cameron[1], Afzal Chaudhry[1], Fiona Hamer[1] and Justin Davies[1]

[1]Cambridge University Hospitals NHS Foundation Trust, Addenbrooke's Hospital, Hills Road, Cambridge, CB2 0QQ, United Kingdom.

Correspondence to Ari Ercole ae105@cam.ac.uk

S1 Definitions and scope

Two legacy forms of unidirectional numeric pager communication remain prevalent in the NHS. The most ubiquitous are short-range messaging pagers which rely on local telecommunication equipment maintained by the institution with signal extending only over the campus. We refer to these as 'bleeps'. Only numeric messages (entered by telephone key-pad) are supported. A much smaller number of long-range pagers are also used. These are provided by national telecommunications providers and are used for messaging staff who need to be contactable both on and off the campus.

Historically we have two parallel bleep systems at CUH: Zetron and Blick. Replacement of both bleeps and long-range pagers was in scope for this project. Of note, a subset of (Blick system) bleeps with voice announcements are also used at CUH for 'emergency' communication (for adult / paediatric / obstetric cardiac arrest, major trauma and fire). These were not in scope since emergency communication does not form part of the national mandate.

S2 Hospital communication and call centre workflow

The bleep systems at CUH were numeric systems. Usual internal workflow was for staff within the hospital to dial the bleep number on dual-tone multi-frequency internal phones and then key in their extension for call-back.

Additionally, the hospital call centre (CUH 'contact centre') provides a hub to facilitate both internal and external calls. The contact centre is on-site and manned 24/7 by CUH agents. The contact centre also maintains a (voluntary) database of staff mobile phone / alternative contact details: calls may be connected if appropriate but such numbers are never disclosed. It also manages rota software which provides detail of which providers are on duty (either by name or by role) and their primary mode of communication, making this available on the hospital intranet for self-service.

S2.1 Historical workflow

Rota database: the database contains the default contact mode for on-duty personnel. This may take the form of on-call bleep numbers (either bleeps for named individuals or 'baton' bleeps) are published for self-service on the hospital intranet. A few Trust mobile phones are also in use and these details are published. Some on-call specialties (e.g. intensive care consultants for admissions) require a phone call as a primary form of communication and this is listed as 'mobile phone, via contact centre.

Internal calls: users may also call the contact centre and ask to speak to providers. The contact centre operative puts the caller on hold and bleeps / pages the requested provider as appropriate with a call-back number. The two calls are then connected if and when they answer.

External calls: external callers may also call the contact centre and ask to speak to providers or to be put through to a specific bleep number. Again, the contact centre operative puts the caller on hold and bleeps / pages the requested provider as appropriate. The calls are then connected if and when they call back.

S2.2 replacement workflow prior to introduction of Secure Chat

Rota database: only provider names or opt-in group names are published so that users can secure chat directly. Other phone workflows remain the same.

Internal calls: users may also call the contact centre and ask to speak to providers. The contact centre operative puts the caller on hold and sends a Secure Chat message to the provider or opt-in group. The message contains a call-back number and, optionally, a brief message. The contact centre operative is able to see if the message has been read. The calls are then connected if and when the requested provider calls back.

External calls: external callers may also call the contact centre and ask to speak to providers or to be put through to a specific bleep number where this is externally known. Again, the contact centre operative puts the caller on hold and sends a Secure Chat message to the requested provider or opt-in group as appropriate. The message contains a call-back number and, optionally, brief details of the caller. The contact centre operative is able to see if the message has been read. The calls are then connected if and when they call back.

S2.3 cutover period workflow

For one week after go-live, the contact centre ran both systems in parallel. I.e. as well as sending a secure chat message, the agent would also send a bleep message with a call-back number.

S3 Secure chat description

Secure chat works similarly to other messaging applications. Any number of users can participate in a chat. Within a chat, it is possible to see when a message has been read and by whom. We have chosen to permanently store all patient related messages in the patient's chart with send / read times. Non-patient related chats are erased after a month. The app is sandboxed and does not track users or access the users phone (except that clinical photographs may also be securely sent if the user grants permission to access the camera).

Secure chat is a user-to-user messaging system. Epic also offers the concept of opt-in groups. We have created these groups are centrally so that names are curated (e.g. "Cardiology ward doctor (ward xyz)", "Surgery urology clinical fellow", "Physiotherapy (surgery)". One or more staff may then opt in to these groups when in these roles. Staff outside the groups can message the group rather than the individual. In this way it was possible to replicate 'baton bleeps'.

S4 Etiquette guide

We compiled an etiquette guide from best practice acquired by Epic from various customers. We do not reproduce it in full for copyright considerations however, in essence the key elements are as follows:

- Allowed modes of communication.
    - Emergency communication (e.g. cardiac arrest, major trauma, fire: voice notification pager).
    - Urgent patient-related communication: Secure chat or phone call (depending on clinical area).
    - Urgent non-patient related messaging: Secure chat or phone call (depending on clinical area).
    - Non-urgent, patient-related messaging: Epic in basket (EHR integrated 'email-like' system for results and general messaging).
    - Non-urgent, non-patient related messaging: NHS email.
- Messaging platforms other than Secure Chat must not be used.
- Where secure chat messages are not responded to in an appropriate timescale, users should try a different means of communication escalate to another member of staff.
- Sending a message without obtaining receiving an urgency-appropriate acknowledgement does not in itself constitute discharge of duty.

S5 Safety surveillance

We created a specific Secure Chat incident type in our Quality Surveillance information System (QSiS). This is a central portal for logging of all quality and safety events for reporting and is culturally well-embedded at CUH. At the time of writing there had been only 15 QSiS tickets raised. 8 of these came from a single service and related to perception that they had been messaged inappropriately. The remaining tickets concerned reports of medical personnel not responding in a timely way to Secure Chat messages. There were no reports of harm to patients.

The implementation group also acted as a conduit for concerns from clinical areas across all divisions of the hospital. There was feedback from sporadic incidents similar to those submitted to QSiS. Again, no harms were reported. There were two second-hand reports of decreased mobile phone battery life which has been cited in [5] as an adoption barrier however these could not be substantiated.

The implementation team is not aware of any incidents where Secure Chat has been found to be a causative factor to date.

S6 Message volumes over time

Figure S1 shows mean messages per month per provider for the organisation as a whole and for selected provider types. Indicative numbers for each provider type were taken to be the number of active employer ('EMP') records in Epic at the time of writing which may marginally overestimate numbers depending on timeliness of offboarding processes. A plateau seems to be apparent some 3 months post-implementation.

It is noteworthy that large volumes of messages were seen as early as January 2022. This was well before cutover and before strong messaging that bleeps and pagers were to be retired. This suggests a high level of user engagement in a number of groups.

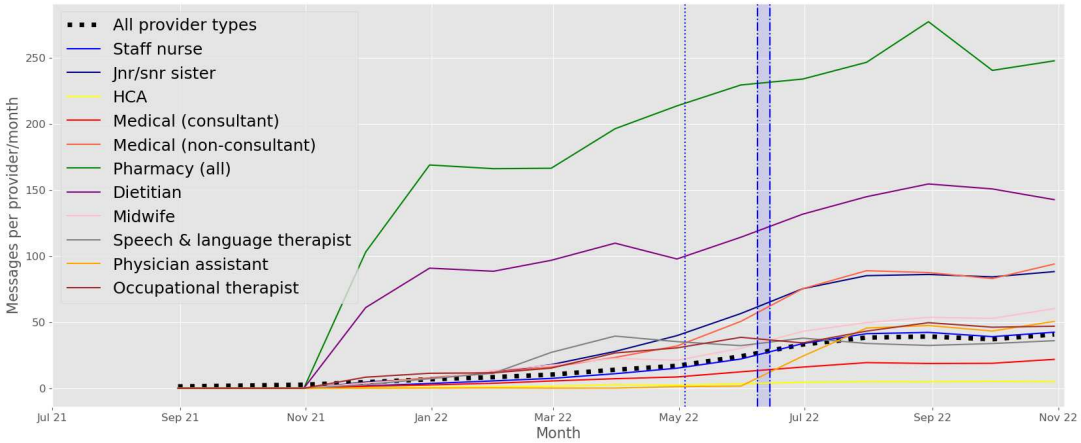

Figure S1 *Messages per provider per month, for selected provider types. A plateau seems to be apparent some 3 months post-implementation. Shaded blue area represents post-go live parallel bleep/secure chat period. Dotted line represents date of delayed initial go-live.*

The equivalent gross number of messages is shown in Figure S2 and reaches approximately 600,000 messages / month across the organisation.

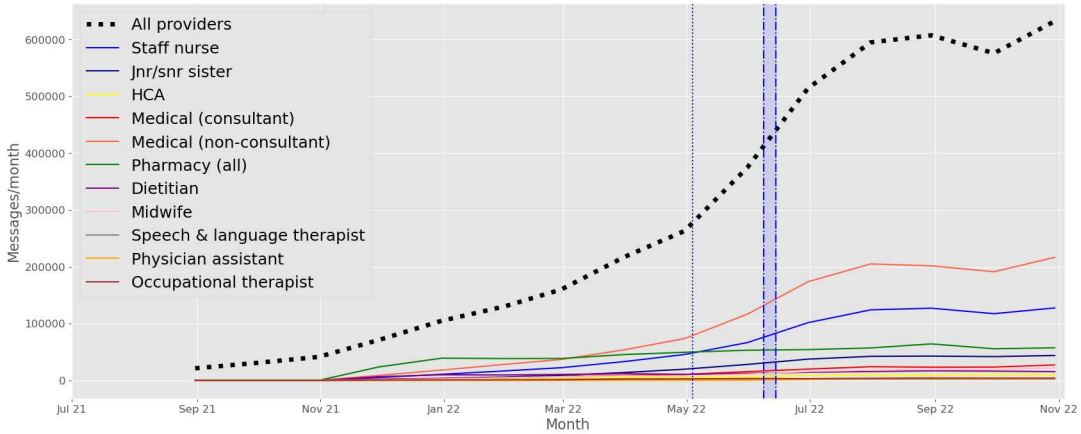

Figure S2 *Gross messages per month (total for the organisation and by selected provider types). Shaded blue area represents post-go live parallel bleep/secure chat period. Dotted line represents date of delayed initial go-live.*

Whilst our bleep system has not been physically retired today, Figure S3 shows a substantial reduction in bleep count for our Zetron system. Whilst we did not capture specific metrics of staff engagement, this is supportive of the notion that staff were content to change from the old system to the secure messaging solution.

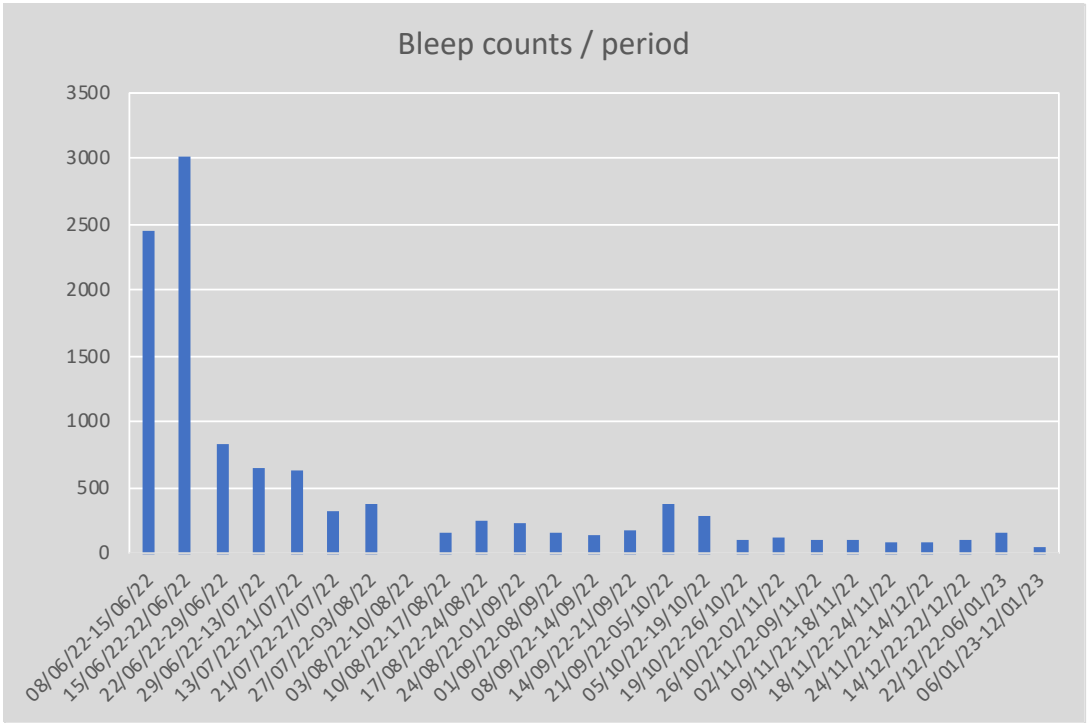

Figure S3 *Bleep counts from our Zetron paging system over time (data for our Blick system were not available). A snapshot audit of the most frequently messaged devices suggested that they were, in fact, largely no longer being actively answered.*

S7 Service desk impact over time

Opt-in groups need to be created centrally by our EHR team. Figure S2 shows opt-in group maintenance activity over time as a proxy for technical maintenance demand.

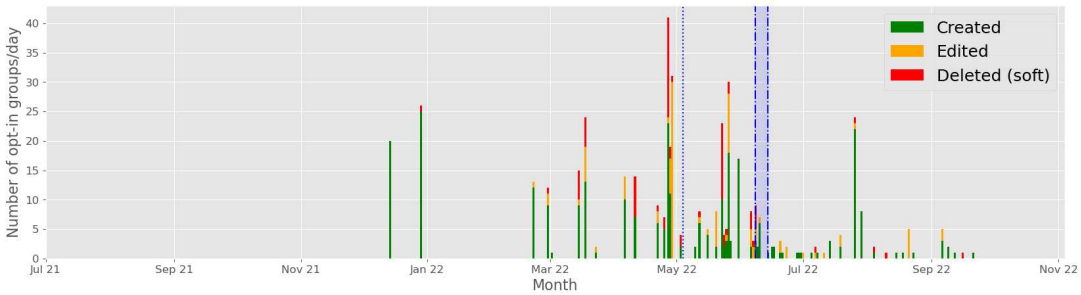

Figure S4 *Opt-in group maintenance activity as a proxy for technical maintenance demand. Shaded blue area represents post-go live parallel bleep/secure chat period. Dotted line represents date of delayed initial go-live. Most of the activity occurred before go-live although spiked after the initial aborted date suggesting that some areas had not properly considered this at that time.*