Strategies for Managing Mobile Devices for Use by Hospitalized Inpatients

Patricia C. Dykes PhD, RN[1,2], Diana Stade[1], Anuj Dalal MD[1,2], Marsha Clements, PhD(c), RN[1], Sarah Collins, PhD, RN[2,3], Frank Chang MSE[3], Anne Fladger, MLS, AHIP[1], George Getty[3], John Hanna[1], Ravali Kandala[3], Lisa S. Lehmann MD, PhD[1,2], Kathleen Leone MBA, RN[1], Anthony F. Massaro MD[1, 2], Eli Mlaver[1], Kelly McNally[1], Sucheta Ravindran[1], Kumiko Schnock PhD, RN[1], David W. Bates MD, MSc[1,2,3]

[1]Center for Patient Safety, Research and Practice, Brigham and Women's Hospital, Boston, MA, [2]Harvard Medical School, Boston, MA, [3]Partners HealthCare, Boston, MA,

Abstract

Despite the potential advantages, implementation of mobile devices and ongoing management pose challenges in the hospital environment. Our team implemented the PROSPECT (Promoting Respect and Ongoing Safety through Patient-centeredness, Engagement, Communication and Technology) *project at Brigham and Women's* Hospital. The goal of PROSPECT is to transform the hospital environment by providing a suite of e-tools to facilitate teamwork among nurses, physicians, patients and to engage patients and care partners in their plan of care. In this paper, we describe the device-related decisions and challenges faced including device and accessory selection, integration, information and device security, infection control, user access, and ongoing operation and maintenance. We relate the strategies that we used for managing mobile devices and lessons learned based on our experiences.

Introduction

The use of technology to manage health and wellness is becoming commonplace. Adoption and use of web-based technologies in everyday life has exploded over the past decade[1,2] and the majority (87%) of American adults use the internet[1]. Many internet users go online to get health information for themselves (72%), or for a family member or friend (50%) [1]. The use of mobile devices is also becoming widespread; 90% of Americans own a cell phone, over half (53%) a smart phone,[3] and increasingly, many own tablet computers. Many Americans report that they use their mobile device as a tool for managing their health. A recent article indicates that there are approximately 90,000 mobile health applications or "apps" available for download [4] and a growing percentage of Americans have downloaded one or more mobile health apps to manage a range of health-related activities[1].

Many consumers are using technology to manage health and wellness, and there is a growing recognition of the need for patient engagement in healthcare[5]. The Health Information Technology for Economic and Clinical Health (HITECH) Act meaningful use program (2009) requires that providers engage patients in their healthcare through the use of technology. A key goal of meaningful use is to make consumers full partners in their care by providing e-health tools that increase access to health information, support activation (e.g., active involvement in their treatment plan), and that help consumers to gain control over their health and wellbeing[6,7]. This has led to provider and healthcare organizations promoting the use of personal health records or patient portals in outpatient settings[8,9]. However, there are limited examples in the literature that describe strategies and e-health tools to provide patients with access to their health information in hospital or inpatient settings. Based on a systematic review of patient engagement

technologies in inpatient settings, Prey et. al. (2014) reported a dearth of published papers describing technologies to engage patients in inpatient settings. The research that has been done in this area is largely confined to pilot and usability studies. None of the papers included in the systematic review described in detail the operational issues related to implementing e-health tools and devices to engage patients, the infrastructure needed for everyday use, and the management issues associated with implementation of these tools in busy acute care settings by a multitude of patients. Early work by Berg et. al. (1999) argue that successful design and implementation of health information technology (IT) applications requires a socio-technical approach; e.g., insight into specific work practices and the dynamic interaction between users and technology in the context of their workflows[1].

In 2014 our team from the Center for Patient Safety, Research, and Practice at Brigham and Women's Hospital (BWH) implemented the PROSPECT (Promoting Respect and Ongoing Safety through Patient-centeredness, Engagement, Communication and Technology) project on BWH medical intensive care (MICU) and oncology units (http://www.partners.org/cird/PROSPECT/Index.htm). PROSPECT is funded by the Gordon and Betty Moore Foundation and BWH. The units (20 ICU beds, 40 oncology beds) were selected to participate based on the GBMF's interest in targeting ICUs and the relatively large percentage of oncology patients that are transferred to the MICU. Our goal is to transform the acute care environment by providing a suite of e-tools to facilitate teamwork among nurses, physicians, patients and to engage patients and their care partners in their plan of care. We hypothesize that through this partnership; we can eliminate preventable harms, make health care more affordable, ensure that patients and families make informed choices about their health care, and improve communication and concordance on goals of care. One component of the PROSPECT project is a Patient-centered Toolkit (PCTK). The PCTK is a web portal that is designed to provide patients and their care partners with the core set of information needed to engage in their plan of care during an acute hospitalization[10-13]. In addition, patients can use the PCTK to message their care team and to provide feedback on their plan of care.

As part of the PROSPECT project, we partnered with our medical librarian to research strategies for ongoing operation and maintenance of bedside devices used by patients in hospital settings and found no peer reviewed literature on this topic. After implementing mobile tablets at each bedside for BWH MICU and oncology patients, we have learned some important lessons. In this paper, we focus on strategies for implementing and managing mobile devices in hospitals and lessons learned based on our experiences from the PROSPECT project. Key questions related to bedside device implementation and management are included in **Table 1**.

Table 1: Key Questions Related to Bedside Device Implementation and Management for the PROSPECT Project	
Device Selection	• What are the technical requirements for bedside devices?
	• What are the end-user hardware requirements for bedside devices?
	• What accessories are needed?
	− Will patients need a tangible keyboard?
	− Are device covers/cases needed?
Device Management	• How will devices be stored (e.g., at the bedside or in central location)?
	• How will devices be cleaned?
Device Related Policies	• How will patients be enrolled?
	• How will care partners be enrolled?
	− What is the process to ensure compliance with institutional policy, IRB (informed consent) and HIPAA regulations?
	− How will user names and passwords be issued?
	• How will information security requirements be addressed?

- How will we prevent devices from theft?

- How will devices be cleaned between patients?

Methods

   We used a socio-technical systems approach[14] to develop the PCTK[12], to identify device requirements, and to identify strategies for ongoing device management. In the 10 months prior to PCTK implementation, we used a range of strategies to gain insight into the MICU and oncology units' work practices into which we would implement the PCTK. We conducted workflow observations, interviews, and focus groups of care team members, patients, and care partners. Based on our evolving set of requirements and the concerns expressed by clinicians and patients, we scheduled meetings with hospital, health information management (HIM), and infection control leadership to address the key questions that arose (**Figure 1**). In addition, we met regularly with information systems (IS) leadership to negotiate integration with existing BWH and Partners HealthCare (PHS) IT systems and to secure approval for device integration and management plans. The details of the iterative, user-centered PCTK development approach are described elsewhere[10-13]. Here we focus on the on the socio-technical aspects of identifying device requirements, the procedures needed for managing bedside mobile devices for the PROSPECT project, and our experiences to date.

Results

   Using the socio-technical systems approach, we identified challenges in terms of device and accessory selection, user access, integration, information and device security, infection control, and ongoing operation and maintenance in the hospital environment. In the sections below we describe the requirements and the implications related to implementing mobile devices at the bedside for patient use.

1. Device type, accessories, storage and user access

      Based on initial feedback from patients and clinicians, we had originally planned to install touch screen, interactive, "smart" devices with built-in keyboards on a moveable arm at the bedside. These devices would support patient access to the PCTK and could be stored flat against the wall when not in use. However, we were unable to implement this approach due to space constraints in the room and the organizational decision to implement a non-touch screen device for use by clinicians in each patient room (device would not be accessible to patients). Therefore we made a decision to use mobile tablet devices. One implication of this decision was that our programmers were developing the PCTK software for use on a Linux, Windows® operating system and a selection of a device that ran on a different operating system, such as Android or iOS, had development implications.

      Once the decision was made to use mobile devices, several issues required consideration including mobile device selection, whether to provide a keyboard, and identification of a device storage strategy that would promote patient and care partner access throughout the hospitalization and ensure the device could be easily charged. We initially identified the following bedside device requirements based on the PCTK technical requirements and user feedback: light weight, optimized screen size, multi-touch screen capability, Bluetooth low energy, and virtual keypad functionality. We explored multiple mobile devices and notebooks and rated each including the iPad Air, iPad mini, Nexus 7 and 10, Surface Pro, ATIC PC Smart, Xperia Series, the Galaxy Note 10.1, Arrows Tab, Macbook Air, LaVie Series, and the CF-LX3. After consideration of infection control (notebook keyboards were difficult to clean) and storage requirements (see below) we made the decision to go with a mobile tablet, rather than a notebook. The Apple iPad Air was the best fit as it met technical and end user requirements, required minimal instruction for use, and received positive feedback for usability from end users. In addition, PHS was using iPads

with patients in other projects and our development team had experience programming on the iOS platform. We purchased 50 iPad Air 2, Wi-fi, 16 GB devices (Apple, Cupertino, CA) for use by patients (and/or designated caregivers) on PROSPECT units to access the PCTK. The total cost for the devices (including the warrantee) was $37,900 ($758 x 50 devices).

We also decided to enclose all devices in a case. Key requirements for device cases were ease of decontamination between patients (no crevices) and preventing damage if the device was dropped. The case needed to be easily gripped, durable, waterproof, and light weight. We reviewed two different cases including the Trent Airbender 1.0 and the military grade Griffin Survivor Case. The Trent Airbender included a keyboard but it was unclear how the keyboard could be cleaned between patients. We selected the Griffin survivor case which was commercial grade and met all of our requirements. The total cost for the cases was $3999.50 ($79.99 x 50 cases). A small percentage of patients we interviewed stated that they needed a tangible keyboard for use with the iPad so we decided to provide accessory keyboards upon request. The keyboards we chose were flexible bluetooth/wireless waterproof keyboards. To date, we have not received any requests for the accessory keyboard. The total cost for the keyboards was $23.98 ($11.99 x 2 keyboards).

The main requirement for device storage and user access was that patients have easy access to the PCTK at all times. This meant that each room would have its own device and charger that are treated as part of the room's equipment and be within reach of the patient from hospital bed. While iPad stands and wall brackets were considered, they were not selected. iPad stands raised concerns about patient falls and wall brackets were ruled out because they did not enable the patients and care partners to use the iPad from anywhere in the room (e.g., the bed, a chair, or couch). Based on bedside workflow observations on inpatient Oncology and MICU units different device housing was developed for each environment. The rooms in the MICU were smaller and had more equipment than the rooms on the

Figure 1a: Oncology unit iPad storage solution. Plastic storage bin is installed on each side of the bedside table to facilitate access from the bed or the chair.

Oncology units. Both environments had over-bed tables but the tables did not have the capacity or potential to hold a mobile device in a practical and sustainable way. We looked at other existing equipment in the rooms and found that
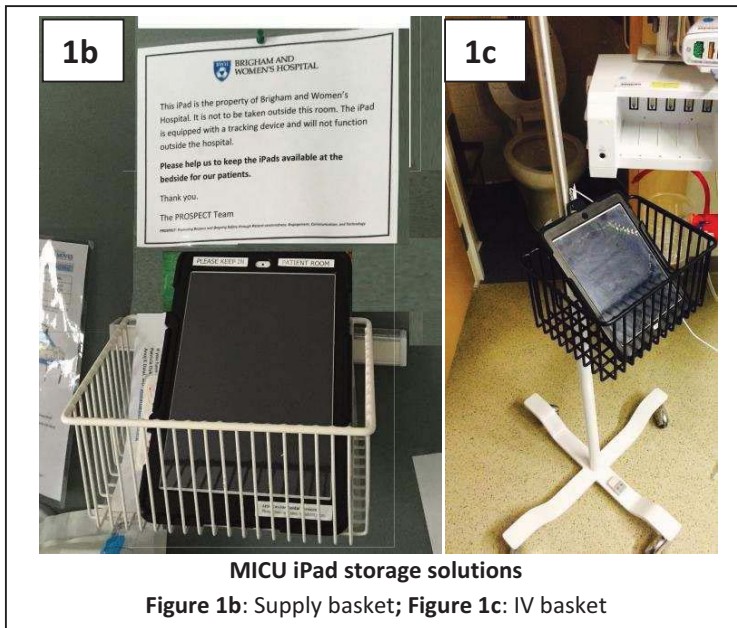
MICU iPad storage solutions
Figure 1b: Supply basket**; Figure 1c**: IV basket

in Oncology there were bedside nightstands. Plastic bins (see **Figure 1a**) were purchased and installed on each side of the nightstand so that patients could easily reach the device from the bed or the chair. The charger was plugged into the wall near the nightstand. This solution has been successful in the Oncology inpatient rooms. We were less successful in the MICU where two different solutions were trialed. The first, which was meant to be temporary, was to utilize the supply basket on the wall above the counter in the rooms where the dressing and other packaged supplies were stored. Under the guidance of the

unit director, baskets were emptied and the devices and chargers were placed in the baskets upon initial installation (see **Figure 1b**). Over time, the baskets were filled back up with supplies in addition to the devices. Meanwhile, our second and long-term solution, recommended by the clinical staff, was to use IV poles with baskets on them which could be placed near the bed but easily wheeled to the side if the space was needed for bedside care (see **Figure 1c**). We installed the poles in each of the rooms and placed the devices in the baskets. Over a few weeks, the poles were either pushed out of the rooms by clinicians, or, they were used for intravenous therapy and not for housing the devices. The clinicians stated that they did not like the extra equipment in the room. Therefore, they have reverted back to using the baskets on the wall to hold the devices. While not ideal, this solution was acceptable because the patients in the MICU are often times incapacitated and it is more common that the Health Care Proxy/care partners use the PCTK. Therefore access from the bed is not always needed.

2. Device integration strategy and device security

We worked with our development team and PHS IS department to identify a device integration strategy that met the needs of the PROSPECT project and was consistent with PHS security policies. First, patients and care partners needed to access personal health information and communicate about their plan of care with the care team; therefore, all devices were connected to the PHS secure wireless network. Second, PHS policy required passwords to be centrally managed and information on devices to be cleared after each patient use. We used an enterprise mobile device management (MDM) solution (AirWatch® by VMware®, Atlanta, GA) to monitor the 50 mobile devices used by approximately 1000 patients/care partners. The MDM software provided remote security controls and reporting capabilities that met both PHS information security policies and HIPAA regulations. Specifically, the MDM software ensured that the iPads were assigned to users, compliance policies were managed, and device tracking was done from a central consol. Thus, any device could be quickly locked down and secured when necessary.

Device and WiFi Issues	Number of Events
Chargers missing/replaced	30
iPads stopped working properly (touch screen functionality failed)	2
iPad disabled from too many logins	4
iPad missing	1
Documented WiFi issues	3

Table 2: PROSPECT Project device and WiFi issues July 2014-February 2015 (N= 50 iPads; 305 patients/care partners)

We also used content management software, Kiosk Pro Lite (Kiosk Group, Inc., Frederick, Maryland) to restrict access on the iPad to the PCTK only.. The iPads were configured by the MDM application to only allow access to the Kiosk Pro Lite software. This prevented data from being downloaded on mobile devices, in compliance with PHS information security policies. All personal health information and patient-provider messaging functionality on

the PCTK were available via secure web services. Therefore, we eliminated the need to clear data on devices between each patient use (although with the AirWatch software, we did have this capability).

Prior to implementation, we were concerned about device theft. We mitigated this threat not only by restricting user access to the PCTK, but also by configuring the MDM software to disallow internet access on all devices outside the PHS firewall. Therefore, the iPads were rendered useless if stolen. We communicated this to patients and clinical staff via signs and weatherproof/laminated, high tack, white, vinyl labels on the back of the iPad case (see **Figure 2**). These labels were also applied to each of the chargers and cords. Thus far, our approach has been successful. Since go-live in July of 2014, only one device has been reported as missing.
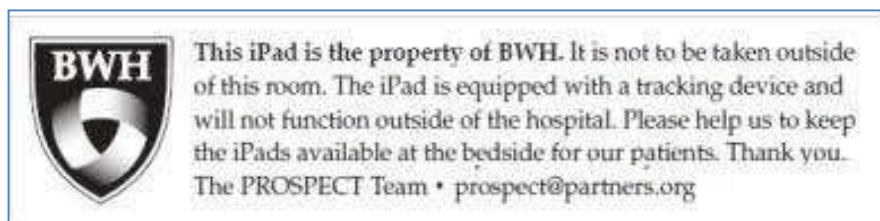

Figure 2: iPad Security Label

We identified issues related to devices and WiFi connectivity after implementation of the PROSPECT project (see **Table 2**). Locking down the iPad devices in kiosk mode did have unintended consequences in that we were unable to leverage the full interactive capabilities of the iPad. First, all pop-ups were suppressed; we were unable to use iframes for some external links or third party apps. This limited the content that we could display. Second, we were unable to use the iPad's notification functionality to display alerts on the lock screen (e.g., when receiving a message from the provider). Finally, patients and care partners could not use the iPads for personal web-browsing, entertainment, email, or video.

Because PROSPECT is a research project, we needed an enrollment strategy that met IRB requirements, PHS information security policies and HIPAA regulations. The IRB required informed consent from all patients and care partners. Patients who had capacity could provide permission for one or more care partners to access their personal health information via the PCTK. For patients without capacity, the healthcare proxy could be enrolled and could use the PCTK on the patient's behalf. First, the process involved securing informed written consent from the patient or health care proxy using the 8-page consent form approved by the IRB. We adopted portal access best practices[15] where possible including providing unique user names and passwords for each user and following a defined permission process. We leveraged existing BWH/PHS policies and practices related to enrollment in the PHS enterprise outpatient portal, Patient Gateway. Once consented, patients/health care proxy completed a PHS access authorization form. An additional form was completed by the patient and care partner for each care partner that the patient identified. Next, we used the PHS administrative portal to enroll patients and care partners. Specifically, users were assigned unique user names (an existing email address) and passwords (assigned by administrative portal and changed by user at the time of the first login).

3. Infection control procedures

During interviews before implementing the PROSPECT project, both patients and clinicians expressed concerns regarding device cleaning procedures. We met with hospital infection control specialists to establish a systematic process for disinfecting devices between patients. To decrease the risk of contamination associated with devices

being carried in and out of rooms, we assigned one device to each patient room.   We communicated the policy that all devices stay in the rooms at all times to hospital staff, patients and care partners. We also posted signs in the patient rooms reminding patients and care partners that the devices were for use in the patient room only. We worked with the BWH environmental services team to implement the approved process for cleaning both iPads and device holders after each patient use along with the other standard equipment in the patient room (see **Figure 3**).

Figure 3: Process for Disinfecting iPad Holders Between Patients

Step 1: Don gloves.

Step 2: Remove iPad from plastic holder.

Step 3: Wipe all of the exposed surfaces of the plastic device holder (outside and inside) using standard disinfectant wipes in use on BWH patient care units. The surface must be wet for the designated time listed for the disinfectant wipe.

Step 4: Check for any leftover stains and repeat as necessary.

Process for Disinfecting iPads between Patients

Step 1: Don gloves.

Step 2: Unplug all connectors from the device and remove any visible stains using standard disinfectant wipes in use on BWH patient care units.

Step 3: Wipe front of iPad using the standard disinfectant wipes in use on BWH patient care units starting at the top corner moving left to right from the top of the device to the bottom of the device. **The process of cleaning the front of the device should take no less than 10 seconds.** The surface must be wet for the designated time listed for the disinfectant wipe.

Step 4: Wipe top of frame and proceed by rotating the iPad in 90 degree steps until all sides of the frame have been cleaned.

Step 5: Turn the device and wipe the back surface starting at the top corner moving left to right from the top of the device to the bottom of the device. **The process of cleaning the back of the device should take no less than 10 seconds.** The surface must be wet for the designated time listed for the disinfectant wipe.

Step 6: Check for any leftover stains and repeat as necessary.

Based on: Albrecht UV, von Jan U, Sedlacek L, Groos S, Suerbaum S, Vonberg RP. Standardized, App-Based Disinfection of iPads in a Clinical and Nonclinical Setting: Comparative Analysis J Med Internet Res 2013;15(8):e176.

Discussion

Despite the advantages, the process of implementing and managing mobile devices in the hospital setting poses multiple challenges. Using a socio-technical approach, we identified a host of issues related to accessory selection, user access, integration, information and device security, infection control, ongoing operation and maintenance. Overall, the socio-technical approach has been useful for identifying and addressing device-related issues and concerns with stakeholders as part of the project planning process. The mobile devices (iPads) have been available on our MICU and Oncology units for over eight months; thus far, the experience has been positive. Enrolled patients and care partners have used the PCTK via hospital-issued iPads to communicate with the care team, contribute to their plan of care, and access their personal health information. To date, we have experienced minimal technical issues with the devices. While we were concerned about device theft prior to implementation, theft of the iPads has not been a problem. Interestingly, missing chargers has been the most common problem, one that we have not solved. Despite our efforts to include stickers on the chargers that indicate that they are BWH property, we have replaced 30 chargers so far (at $19.00 for adaptor and $29.99 for 6ft cord equates to $1,469.70 or an additional $200

per month in charger replacement costs). We are currently working on a secured solution for managing the device chargers.

We learned throughout the project that device-related decisions can have unintended consequences. As noted, we made the decision to use mobile devices after we learned that we could not install interactive, "smart" devices on a moveable arm at the patients' bedside. This decision required some rework by our software developers to optimize the PCTK for use on the iOS operating system. Additionally, we had to address mobile device storage, charging, infection control, and security issues within our original timeline. Using a socio-technical approach, we worked through these issues with stakeholders and arrived at solutions in parallel with the PCTK software development. Some of the solutions were more successful than others. For example, establishing a device storage protocol so that devices were accessible by patients, continuously charged, and not in the "way" of clinical staff was difficult. We found that there was not a single best way to meet these requirements across units and we implemented two different solutions, one more successful (oncology units) than the other (MICU).

Our decision to lock iPads into kiosk mode facilitated information and device security, but it also led to an unexpected loss of access to MedlinePlus content. Initially, we linked to MedlinePlus educational content for test results, medications, and problems. We chose MedlinePlus because the content was at a consumer level of health literacy, had broad content coverage, and did not have advertisements. MedlinePlus contained licensed content from other sources and their license agreements did not permit framing of their content from their site. Medline Plus started blocking the framing of educational content in December 2014, several months into our project and our patients lost access to all of the educational content (e.g., all of the infobuttons "broke"). We quickly changed to other content sources and we started the process of implementing the web service version of MedlinePlus Connect so that we can once again use that content.

Our information security requirements have been a challenge at times. PHS requires encryption of all mobile devices that display patient health information including a lock screen and passcode. The lock screen appears when the battery power is less than 20% or if the device is restarted (e.g., the battery completely dies and the device is then plugged in). Even though the devices are in kiosk mode, a separate passcode is required to bypass the lock screen. When the lock screen appears, it can only be unlocked with the assistance of our research staff.

Cost represents a barrier to widespread adoption of mobile devices. In addition to the hardware and software costs, the administrative infrastructure needed to keep track of the devices and to enroll patients is significant. For the PROSPECT project, devices were managed by the research team. Sustainability outside the context of a research project will require an organizational approach to systematically address the issues identified by our team. Building this infrastructure would require institutional commitment and resources. One lower cost strategy that would mitigate access, device security, infection control, and operational concerns is to allow patients and care partners to access the PCTK on their own mobile device. A "bring your own device (BYOD)" strategy has much appeal as hospitals are essentially liberated from concerns related to removing prior data and configuring access to device after each patient use, monitoring and tracking devices to prevent theft, cleaning devices per hospital infection control protocols, and maintaining devices and accessories (e.g., losing chargers). A BYOD strategy should improve accessibility from the locked screen as patients and care partners would not have to remember additional passwords. To ensure privacy and security of patient health information, a BYOD strategy would require access via web-based patient portal applications with standard username and password authentication requirements. The use of native apps downloaded onto the mobile device to access web-based patient portal applications should enhance interactivity (i.e., by leveraging device specific API's such as push notifications), as long as patient data resides on secure, HIPAA-compliant servers. Ideally, patients and care partners would download an app onto their mobile device at their convenience (e.g., as part of the hospital admission process). Additionally, such a strategy may increase flexibility for access by care partners who are unable to be at a patient's bedside. Finally, with a BYOD strategy providers could "prescribe" mHealth apps that serve to engage patients in understanding and managing their care during recovery and after leaving the hospital[16]. However, this requires a rigorous mHealth app certification and

approval process to be in place[17]. Next steps for the PROSPECT project include developing a BYOD strategy that will improve patient access to the PCTK on all BWH inpatients units.

There are several limitations associated with this project. We implemented the devices at a single hospital and within the context of a research study. It is not known how generalizable our experience is to other hospitals or healthcare settings. In addition, we have been using research assistants to enroll patients and track the devices. More research is needed to evaluate how these device-related functions could be integrated into a hospital environment without this level of support.

To our knowledge, this is the first report of lessons learned related to implementing mobile devices at the bedside for an extended period of time. We hope that with this paper, we have started the conversation and that others will publish their experiences so that barriers to implementation of e-health tools will be identified and addressed and these tools can be used more widely to engage hospitalized patients.

References

1. PewResearch. Health Fact Sheet. 2013. http://www.pewinternet.org/fact-sheets/health-fact-sheet/.

2. PewResearch. America's Online Pursuits: Information Utility Activities. 2003; http://www.pewinternet.org/2003/12/22/part-3-information-utility-activities/.

3. PewResearch. Digital differences. 2012; http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Digital_differences_041312.pdf.

4. Jahns RG. The market for mHealth app services will reach $26 billion by 2017. Research2Guidance. 2013. www.research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017.

5. IOM. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington, DC: Institute of Medicine;2001.

6. CMS. CMS EHR Meaningful Use Overview. 2012; http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html. Accessed May 6, 2012.

7. HHS.GOV. Electronic Health Records and Meaningful Use. 2011; http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__meaningful_use_announcement/2996. Accessed October 3, 2011.

8. Ancker JS, Silver M, Kaushal R. Rapid growth in use of personal health records in New York, 2012-2013. Journal of general internal medicine. Jun 2014;29(6):850-854.

9. Garrido T, Meng D, Wang JJ, Palen TE, Kanter MH. Secure e-mailing between physicians and patients: transformational change in ambulatory care. The Journal of ambulatory care management. Jul-Sep 2014;37(3):211-218.

10. Dykes PC, Stade D, Chang F, et al. Participatory Design and Development of a Patient-centered Toolkit to Engage Hospitalized Patients and Care Partners in their Plan of Care. Paper presented at: AMIA Fall Symposium.; Nov 14-18, 2014; Washington DC.

11. Caligtan CA, Carroll DL, Hurley AC, Gersh-Zaremski R, Dykes PC. Bedside information technology to support patient-centered care. International journal of medical informatics. Jul 2012;81(7):442-451.

12. Dykes PC, Carroll DL, Hurley AC, et al. Building and testing a patient-centric electronic bedside communication center. Journal of gerontological nursing. Jan 2013;39(1):15-19.

13. Ohashi K, Caligtan CA, Benoit AN, et al. An electronic patient risk communication board. Nursing informatics ... : proceedings of the ... International Congress on Nursing Informatics. 2012;2012:311.

14. Berg M. Patient care information systems and health care work: a sociotechnical approach. International journal of medical informatics. Aug 1999;55(2):87-101.

15. Sarkar U, Bates DW. Care partners and online patient portals. Jama. Jan 22-29 2014;311(4):357-358.

16. Greysen SR, Khanna RR, Jacolbia R, Lee HM, Auerbach AD. Tablet computers for hospitalized patients: a pilot study to improve inpatient engagement. Journal of hospital medicine. Jun 2014;9(6):396-399.

17. Powell AC, Landman AB, Bates DW. In search of a few good apps. Jama. May 14 2014;311(18):1851-1852.