Distraction: an assessment of smartphone usage in health care work settings

Abstract: Smartphone use in health care work settings presents both opportunities and challenges. The benefits could be severely undermined if abuse and overuse are not kept in check. This practice-focused research paper examines the current panorama of health software applications. Findings from existing research are consolidated to elucidate the level and effects of distraction in health care work settings due to smartphone use. A conceptual framework for crafting guidelines to regulate the use of smartphones in health care work settings is then presented. Finally, specific guidelines are delineated to assist in creating policies for the use of smartphones in a health care workplace.

Keywords: smartphone, health care, distraction, workplace, mobile apps, health informatics

Introduction

Smartphones are becoming central to our everyday lives. They serve as a means to fulfill tasks both at work and home. The market penetration of these devices is rising in every industrial sector and professional field. For example, in 2009, 64% of America’s physicians used smartphones.1 This number is predicted to reach 81% by the end of 2012.1 In professional settings, pervasive use of these devices presents many challenges. In health care work settings, they could become privacy and security risks, as well as a source of distraction for the workforce. Hence, it may be prudent to establish policies to guide employees using smartphones at work to prevent any abuse and overuse.

In this practice-focused research paper, we looked at health care-related software applications available across major smartphone platforms. Smartphone software applications are becoming increasingly popular for both health care consumers and providers.2 Findings from existing work illustrate that smartphones are a significant source of distraction for decision-based activities such as driving, classroom learning, and work-related tasks. Similarly, in health care work settings, these devices pose a great risk. As is shown in the examples presented in this paper, mistakes and omissions in health care work settings could have fatal repercussions. Distraction and errors could also put privacy and security at stake. We conclude that every health care organization should address the use of smartphones at workplaces; we present a framework to devise guidelines for the use of smartphones in health care work settings. We also propose a comprehensive set of guidelines for regulating the use of smartphones in work-related tasks while maximizing efficiency.
Smartphones and software applications

A smartphone could be defined as a mobile phone that has additional functions similar to personal digital assistant devices. Examples of smartphones include Apple® (Cupertino, CA) iPhone®, 3G, 3GS, 4 and 4S, Google (Mountain View, CA) Android™ based devices like Samsung Galaxy S(R) II and HTC One V, RIMS® (Waterloo, ON, Canada) BlackBerry® devices like BlackBerry® Bold™ and BlackBerry® Curve™ and Microsoft Windows® (Redmond, WA) based devices like Nokia Lumia 900 and HTC TITAN II™. A smartphone application (app) is defined as a software application that runs on a smartphone or other portable device.2 Apps are run on smartphones and media tablets with or without Internet connectivity. Wasserman3 suggested that successful mobile app software involved user experience, explicit and implicit/latent functional requirements, underlying processes, right architecture, and platform portability. Smartphone apps are compact software programs that perform specific tasks for the mobile user. There are two types of smartphone apps: (1) the native app that must be installed on the device or that arrives preinstalled on the phone and (2) the Web app that resides on a server and is accessed via the Internet.4

According to the International Data Corporation,5 over 300,000 smartphone apps were developed between 2007 and 2010. The organization further stated that smartphone app revenues would experience more than 60% compound annual growth through 2014, worldwide. An interesting trend, however, exists in the smartphone app market. The average cost of downloading apps is going down.6 This is shown in Table 1. Smartphone apps can be bought from myriad sources. Some examples include Apple® App StoreSM, Android™ Market, BlackBerry® AppWorld™, Nokia (Espoo, Finland) Ovi Store and Windows® Phone Marketplace. In 2012, Apple® Inc reported that its app store offered approximately 550,000 apps, divided into 21 categories.7 In the same year, Google Inc claimed that there was an increase in app consumption.8 Furthermore, Google’s Android™ Market media store users downloaded about 2.4 billion apps in the third quarter of 2011. However, Suthoff9 reported that even though a large number of apps might be sampled, about a quarter of them are discarded after initial use.

According to the Nielsen Company,10 the popular categories of smartphone apps include games, music, social networking, news, weather, maps/navigation, video/movies, entertainment/food, sports, communication, banking/finance, shopping, productivity, and travel/lifestyle. A detailed breakdown of smartphone use has been presented by Gartner Inc.11 It projects that, by 2012, the top ten smartphone apps would include money transfer, location based services, search, browsing, health monitoring, mobile payment, near-field communication service, advertising, Internet messaging, and music. This prediction may not turn out to be completely true, but it indicates that smartphone apps play a big role in modern society. Furthermore, cellular phone ownership in 2011–2012 showed that the number of smartphone owners has gone up, from 35% in 2011 to 46% in February 2012,12 while the number of nonusers of smartphones has decreased from 48% to 41%.

A study by ComScore Inc,13 conducted between October and December 2011, showed that the total mobile audience (age: 13+ years) that used a browser or an app or performed a download operation was 47% in the USA, 41% in Europe, and 37% in Japan. A majority of the mobile audience used their mobile device cameras to take photos: 52% in the USA, 58% in Europe, and 63% in Japan. Similarly, of the mobile audience (age: 13+ years), 42% in the USA, 31% in Europe, and 58% in Japan accessed news and/or information through their mobile devices. Like the aforementioned Gartner Inc11 report, the data from ComScore13 identified the mobile device audience (age: 13+ years) as using their mobile devices for tasks such as search, download, browsing, messaging, email, social networking, gaming, watching television, music/radio, banking, travel services, and location-based services/GPS. These findings demonstrate that smartphone app usage impacts many aspects of our lives. Smartphone apps are becoming the primary way we get and use information.

### Software applications for health care

Across major smartphone platforms, we noticed some common app categories for health care: health and fitness, medical, and lifestyle. In 2011, Dolan14 reported that there were about 9000 medical, health, and fitness apps available for the iPhone alone. This number has multiplied dramatically. We conducted a search on Apple’s® iPhone® App StoreSM, which yielded 5102 apps when the term “medical” was searched.

<table>
<thead>
<tr>
<th>App Stores</th>
<th>Apple® App StoreSM</th>
<th>BlackBerry® AppWorld™</th>
<th>Nokia Ovi Store</th>
<th>Android™ Market</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of apps</td>
<td>300,000</td>
<td>18,000</td>
<td>130,000</td>
<td>25,000</td>
</tr>
<tr>
<td>Price change % (Jan 2010–Jan 2011)</td>
<td>-12</td>
<td>-24</td>
<td>1</td>
<td>-29</td>
</tr>
</tbody>
</table>
The search terms “health” and “fitness” yielded 7898 apps. An Google’s Android™ Market media store search showed 4290 apps when we searched for “medical” and 9522 apps when we searched for “health and fitness.” A search on RIMS® BlackBerry® AppWorld™ resulted in 1621 apps when we queried “health and fitness” in the search box. We noticed that the apps were further tagged as “fitness,” “health and diet,” “health care services,” and “medical guides.” These tags were indicated next to each search result. There were no results for “medical.” The Nokia Ovi Store yielded 12 apps for “medical” and 50 apps for “health and fitness.” These searches were conducted on April 23, 2012. We verified each result to ensure that the apps counted were in accordance with the searched keywords. We excluded the apps that did not seem to concur with the searched keywords.

It is noteworthy that major companies in fact sponsor some of the popular health care apps. For instance, The CareConnector® for iPhone® – which provides contact information for health care providers, prescription details, insurance policy details, and so forth – is sponsored by Johnson & Johnson Consumer Products Company, Inc (New Brunswick, NJ, USA). TYLENOL® (Fort Washington, PA, USA) sponsors TYLENOL® PM Sleep Tracker, which tracks sleeping patterns. Merck & Co, Inc (Whitehouse Station, NJ) sponsors iChemoDiary, which helps one cope with the modalities of chemotherapy, for instance, by tracking negative effects, recording log appointments, and maintaining the treatment calendar. In 2011, Kalorama Information,15 a health care market-research publisher, reported that the market for mobile medical apps was worth about US$50 million. They claimed that this number competed with popular app categories such as games, entertainment, social networking, and navigation. With the increasing number and variety of apps available across all platforms, it is plausible that there is an increasing demand for smartphones in health care.

It can be argued that the growth in the number of apps related to health care indicates that there could be substantial use of these apps in health care work settings. In order to ensure that this use does not become a cause of errors and inefficiencies, health care organizations must consider creating coherent and practical policies for the use of smartphones in the workplace and beyond.

Distraction from tasks involving decision making
Cellular phones, including smartphones, are known to be detrimental to cognitive performance. Their use increases reaction time, reduces focus, and lowers performance of tasks needing mental concentration and decision making. In 2010, The US National Safety Council16 estimated at least 23% of all traffic crashes per year – at least 1.3 million crashes per year – involve cellular phone use. Parker-Pope17 established that cellular phones impact attentiveness, and cause inattentional blindness. Users become so engrossed in their cellular phone that, even though they may be looking at their surroundings, nothing actually registers. Shelton et al18 asserted that we can only attend to a limited amount of information at any given moment, and that using the cellular phone reallocates attention resources. A user preoccupied by the cellular phone is distracted from the other, primary task that he or she is performing. Hyman et al19 investigated the effects of divided attention on walking while using a cellular phone. It was found that users walked more slowly, changed directions more frequently, and were less likely to acknowledge others, as compared to those listening to MP3 players, walking in pairs, or walking alone. They also realized that cellular phone users were less likely to register any unusual activity along their path. Madden and Lenhart20 reported that 52% of cell-owning teens, ages 16–17, said they had talked on a cellular phone while driving. Additionally, 48% of all teens, ages 12–17, said they had been in a car when the driver was sending a text message.20 Strayer et al21 observed that a person using a cellular phone while driving and a person driving with a blood alcohol-level above the legal limit have a similar chance of being involved in a traffic accident. Through simulated studies, Lesch and Hancock22 established that simultaneously driving and using a cellular phone caused brake-response time delays of approximately one-third of a second for older drivers, aged 55–65 years, and of one-tenth of a second for younger drivers, aged 25–35 years. Similarly, stopping times decreased by half a second for older drivers and by one-tenth of a second for younger drivers. Ma and Kaber23 proved that having cellular phone conversations while driving caused deleterious effects on driving and increased drivers’ mental load. The secondary cellular phone task competed for the driver’s attention, diverted his or her focus, and lessened accurate knowledge of the driving circumstances. It can be concluded that cellular phone use, including smartphones, could be a source of distraction during other decision-making tasks.

Distraction from health care caused by smartphones
As highlighted in the previous sections, mobile health care applications are numerous and widely available. In 2010, Dolan24 reported that close to 50% of the health-related
apps were targeted towards medical professionals, such as physicians and medical students. Halamka24 observed that mobile devices, including smartphones and tablets, could be used in conjunction with clinical information systems. Gold25 reported that smartphones were a distraction to doctors working in hospitals. Care needs to be taken to ensure that they are not a hindrance. This can be achieved by establishing best practices and policies for using such devices in health care work settings. In health care, even a small mistake can prove fatal. Halamka24 reviewed a case where a medical resident forgot to stop an anticoagulation medication for a postoperative patient. The medical resident was distracted by a text message she received on her smartphone, which distracted her, and she forgot about her primary task.

Westbrook et al26 found that each interruption to medical care workflow at an Australian hospital was associated with a 12.1% increase in procedural failures and a 12.7% increase in clinical errors. Wu et al27 reported that physicians’ smartphones received, on average, 21.9 emails and 6.4 telephone calls while sending out 6.9 emails and initiating 8.3 telephone calls over a 24-hour period. Negative outcomes of smartphone usage included interruptions and discordance between what doctors and nurses considered urgent.27 Nurses perceived a worsening of interprofessional relationships due to overreliance on messaging by text, resulting in a decrease in verbal communication.27 Unprofessional behaviors were observed in the use of smartphones by residents.27 Smith et al27 reported that 55.6% of 439 perfusionists admitted that they used a cellular phone, and 49.2% agreed that they had sent text messages while performing a cardiopulmonary bypass. Some 7.3% of the perfusionists admitted that the cellular phone had a negative impact on their performance. And 33.7% said they had seen another perfusionist distracted by the cellular phone. Of those surveyed, 21% reported having accessed email, 15.1% having used the Internet, and 3.1% having used social networking sites. A 2012 report by Facebook28 reveals that the user base at the end of March 2012 stood at 901 million active users from all walks of life. Thus, it is plausible that many health care providers are also among the active users.

Rosenfield et al29 recognized that smartphones could facilitate learning, treatment, and communication by capturing interesting diagnostic images or recording procedures, but that they could also be disruptive and distracting. They contended that it would be difficult to find a health care team wherein at least one member was not preoccupied on their phone during rounds. Rosenfield et al29 affirmed that smartphones tended to compromise patient privacy and confidentiality and users tended to forget that sensitive information was being let out in a public setting. Hence, technology in itself is neutral, but its use may not be. Similarly, Visvanathan et al30 observed that mobile communication technology comes with risks such as electromagnetic interference, loss of confidentiality and data security, distraction/noise, infection control, and cross-contamination. Smartphone usage while performing medical tasks raises safety concerns. These concerns can be addressed by regulating the use of smartphones in health care work settings.

Alsos et al31 conducted a study to assess the negative effects of information technology (IT) on doctor–patient dialogue and established that the collaboration was best when the doctors were using a paper chart to communicate with their patients. They observed that personal digital assistants or laptops inhibited aspects of essential communication such as eye contact, gestures, visibility of actions, and verbal and non-verbal contact, which was a hindrance to quick and efficient information retrieval and communication. Cain32 reported that health care and other organizations were concerned about the time and attention employees allocated to social media discourse while on the job. For most organizations, such distractions lead to loss of productivity, but in health care, it could result in medical errors, which in turn might have serious repercussions. Cain32 established that accessing social media via smartphone while performing work-related tasks was more problematic than accessing social media via computer, because the smartphone was portable and hence more likely to be a constant source of disruption. Similarly, McBride’s33 analysis indicated that cellular phone users were so engrossed in this activity that they were often unaware of their own misuses and might not realize they were distracted. It was also observed that the reduced visual field or diverted attention caused by cellular phones used during medical procedures might result in the health care provider not recognizing potential complications. Also, if an accident were to occur, an attorney could obtain telephone records and try to prove medical negligence. McBride33 acknowledged that modern devices had great potential to reduce risks, but concluded that operating the device could be distracting.

Apart from being a distraction, use of smartphones in health care facilities presents contamination, infection, and hygiene risks. Brady et al,34 Hassoun et al,35 Braddy and Blair,36 and Al-Abdalall37 showed that mobile devices used in health care settings could entail a high level of microbial contamination. Additionally, studies by Halamka44 and Visvanathan et al38 showed that the electromagnetic radiation from the mobile devices not only could hamper the functionality of patient devices such as pacemakers, but also could interfere
with other medical equipment. Ogg\textsuperscript{38} expressed concern over hospital staff using cellular phones in the operation room and believed that bacteria-laden devices could possibly cross-contaminate the practitioner’s hand. Along the same lines, a study conducted at a health care organization in Ireland to test the bacteria-carrying potential of cellular phones showed that, of the 70\% cellular phones tested for bacteria that could cause infection, 96\% were contaminated and 15\% had bacteria known to cause health care-associated infections. Similarly, Cain\textsuperscript{39} reported that pharmacy and medical students lacked good judgment when sharing information and presenting themselves online, and believed that information published via social media was irrelevant to the workplace. Furthermore, Cain\textsuperscript{39} reported that of over 34,000 health care employers surveyed, only 25\% had a formal policy on using social media at work. Warwick\textsuperscript{40} observed that although in some areas smartphones may result in the increased responsiveness, efficiency, and productivity of employees, they could also increase risk to security and privacy. Completely banning the mobile devices in a workplace is not an option, since this in turn may lead to temporal attention detachment and intentional nonadherence. A smartphone usage policy for health care work settings that addresses the issues presented above could help alleviate the associated risks.

\section*{Framework}

We propose that health care organizations perform analyses of the strengths, weaknesses, opportunities, and threats (SWOT) analyses to judge if a smartphone app adds value to their patient care and other services. Furthermore, SWOT analyses for a larger number of apps could form the blueprint for creating a framework for smartphone usage policy in health care work settings. As an illustration, we conducted SWOT analyses for the top iPhone\textsuperscript{®} apps targeted at nurses.\textsuperscript{41} The apps reviewed are shown in Table 2. The results are presented in Table 3.

\begin{table}[h]
\centering
\caption{List of 15 iPhone\textsuperscript{®} apps analyzed using the strengths, weaknesses, opportunities and threats approach.}
\begin{tabular}{|l|l|l|l|}
\hline
15 iPhone\textsuperscript{®} apps included in SWOT analysis & PALS Advisor 2012 & ACLS Advisor 2012 & Epocrates\textsuperscript{®}  \\
& iCharts, Inc\textsuperscript{®} & MedCalc Software bvba & iMurmur 2.0 \\
& VisualDx\textsuperscript{®} & Memos & NURSE Central\textsuperscript{TM} \\
& Infuse & Perfect OB Wheel & Lytes  \\
& STAT\textsuperscript{®} & Nursing Central\textsuperscript{TM} \\
& Lytes & Perfect OB Wheel & Nursing Central\textsuperscript{TM} \\
\hline
\end{tabular}
\end{table}

Warwick\textsuperscript{41} suggested that smartphones that are not compliant with basic security and malware protection policies should not be allowed to access the company network. Organizations should take measures that prohibit unauthorized/unlawful smartphones from accessing their network and information. It is also important to establish who owns the data being downloaded on an organization’s network. In cases where the phone is provided by the organization itself, it is important to establish who owns the data stored on that phone. Smartphone technology is continuously evolving, and institutions need to ensure that their security and privacy measures keep up with any changes. Warwick\textsuperscript{41} assessed how smart devices, including smartphones, are likely to force a rethinking of information security functions’ entire approach to deploying controls and solutions. A one-size-fits-all approach is not applicable when devising guidelines and policies for secure smartphone usage. Each health care organization has to introspect, analyze their employees’ data needs and phone usage, and realize their organization’s demands for this type of communication and while coming up with a set of relevant guidelines.

Health care is all about patient care, which is personal and which requires physical interaction and direct communication. Hoppel\textsuperscript{42} held that when health care professionals entered a room to see a patient, they had to always keep in mind that the patient was the most important person in the room. Policies need to ensure that personal messages or any kind of interruptions via smartphones or any electronic gadgets are avoided. Health care providers need to set up smartphone usage policies to make sure that they provide a secure environment for their patients.

Edwards et al\textsuperscript{43} recommended developing solutions that would result in enhanced interclinician communication and reduced interruptions, or interruptions deferred to more appropriate times. Furthermore, Lo et al\textsuperscript{44} concluded that smartphone technology was well received among health care providers, especially because they could be useful in both urgent and non-urgent scenarios. They also recommended that future interventions should tackle the following issues: (1) suitability of these smartphone features and (2) appropriate use in different communication and situational contexts. Sweeney\textsuperscript{45} put forth guidelines to regulate the use of smartphones in corporate settings to ensure best-practices work ethics and to take a platform-agnostic approach. Some of Sweeney’s guidelines\textsuperscript{45} that could be implemented by health care institutions are the following:

1. Since smartphone users’ identities and the information on the phone can be inappropriately used, stolen, hacked, and shared,
device-identification technology and security features should be used to associate smartphones with their users. This can be extended to include features where all sensitive information can be remotely erased and/or locked and managed to prevent misuse. Encrypting data, password protection, and smartphone-locating features may prove to be beneficial.

2. Establish a SSL VPN, a technology that allows remote locations to securely access a private network.

3. Scan all smartphone traffic on their network.

4. Comprehensively scan and prioritize smartphone traffic in real time.

5. Ensure high-security Wi-Fi connections.

6. Use application technology intelligence and control technology to extend firewalls to identify, categorize, control, and report application usage on the network.

7. Limit bandwidth-consuming traffic like YouTube™ (San Bruno, CA, USA) and NETFLIX.

8. Protect the converged voice-and-data communications that smartphones today feature.

9. Decide which smartphones should be allowed on the network.

Shinder also presented some actions regarding legal issues to consider while formulating company policies to govern smartphone use:

1. Allot a separate phone for business use – with a signed agreement – that should be used for work-related matters. In such a scenario, the employer purchases and retains the ownership of the phone, and may decide if the phone should or not be used for personal tasks.

2. Decide who owns the data stored on company-issued devices.

3. Have GPS functionality to track down company owned devices.

4. After assessing the legal repercussions, install software on organization-owned phones to record and/or listen to conversations, remotely read call logs, emails, and SMS messages.

5. Police, establish, and clearly communicate the legal repercussions of using company phones on a network to attack, hack, access, and download porn, to harass someone, or to commit any illegal act.

Based on the aforementioned recommendations, we recommend that health care workplaces: (1) set up hardware and software firewalls; (2) prevent mass emails to addresses outside the company network; (3) block communication to popular/known advertising and marketing websites; (4) block websites that have low security; (5) set up email services specific to the institution to minimize the use of personal email; (6) regulate the use of apps while on the network; (7) appropriately employ updates and patches in a timely manner; (8) set up organizational rules for password strength and composition; (9) encourage employees to regularly change their password; and (10) train existing and new employees about IT norms, security concerns, and expectations.

It also becomes imperative to consider that the use of smartphones and similar mobile devices cannot be completely restricted, and thus that the guidelines should address the distractions that result from their use in health care work settings. Furthermore, health care providers need to ensure that patient-care standards are not compromised by the use of these devices. Based on the concerns presented in our review, the following solutions can be used as a starting point or example while formulating such guidelines:

1. Create specific zones for the professionals to use their smartphones, with Wi-Fi hotspots. This will minimize the use of smartphones in other sensitive/restricted areas. These zones could be integrated with cafes or break rooms to ensure that the health care professionals are not preoccupied with work-related activities.

### Table 3 Combined results of strengths, weaknesses, opportunities, and threats (SWOT) analyses performed on 15 iPhone applications (apps) geared towards health care providers

<table>
<thead>
<tr>
<th>Strengths (S)</th>
<th>Weaknesses (W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Convenient: Information at your fingertips</td>
<td>1. Need to be tech-savvy</td>
</tr>
<tr>
<td>2. Designed and maintained by medical professionals</td>
<td>2. Need to own a smartphone</td>
</tr>
<tr>
<td>3. Regularly updated with new health care related data</td>
<td></td>
</tr>
<tr>
<td>4. Easy to use</td>
<td></td>
</tr>
<tr>
<td>5. Allows health care professionals to connect to consumers/patients directly</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities (O)</th>
<th>Threats (T)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Standardized/digitized format for storing data</td>
<td>1. Compromise patient privacy and security: unsure who else has access to his information beside the doctor and hospital</td>
</tr>
<tr>
<td>2. Allows health care professionals to communicate at a global level</td>
<td>2. Users might access it across multiple devices, which poses data-privacy risks</td>
</tr>
<tr>
<td>3. Allows health care professionals to communicate at a global level</td>
<td>3. Source of distraction – alerts, beeps, reminders can be distracting</td>
</tr>
<tr>
<td>4. Limits bandwidth-consuming traffic like YouTube™ and NETFLIX.</td>
<td>4. Interrupts continuous communication with the patient</td>
</tr>
</tbody>
</table>

5. Protect the converged voice-and-data communications that smartphones today feature.

9. Decide which smartphones should be allowed on the network.

Shinder also presented some actions regarding legal issues to consider while formulating company policies to govern smartphone use:

1. Allot a separate phone for business use – with a signed agreement – that should be used for work-related matters. In such a scenario, the employer purchases and retains the ownership of the phone, and may decide if the phone should or not be used for personal tasks.

2. Decide who owns the data stored on company-issued devices.

3. Have GPS functionality to track down company owned devices.

4. After assessing the legal repercussions, install software on organization-owned phones to record and/or listen to conversations, remotely read call logs, emails, and SMS messages.

5. Police, establish, and clearly communicate the legal repercussions of using company phones on a network to attack, hack, access, and download porn, to harass someone, or to commit any illegal act.

Based on the aforementioned recommendations, we recommend that health care workplaces: (1) set up hardware and software firewalls; (2) prevent mass emails to addresses outside the company network; (3) block communication to popular/known advertising and marketing websites; (4) block websites that have low security; (5) set up email services specific to the institution to minimize the use of personal email; (6) regulate the use of apps while on the network; (7) appropriately employ updates and patches in a timely manner; (8) set up organizational rules for password strength and composition; (9) encourage employees to regularly change their password; and (10) train existing and new employees about IT norms, security concerns, and expectations.

It also becomes imperative to consider that the use of smartphones and similar mobile devices cannot be completely restricted, and thus that the guidelines should address the distractions that result from their use in health care work settings. Furthermore, health care providers need to ensure that patient-care standards are not compromised by the use of these devices. Based on the concerns presented in our review, the following solutions can be used as a starting point or example while formulating such guidelines:

1. Create specific zones for the professionals to use their smartphones, with Wi-Fi hotspots. This will minimize the use of smartphones in other sensitive/restricted areas. These zones could be integrated with cafes or break rooms to ensure that the health care professionals are not preoccupied with work-related activities.
2. Set up to-do checklists in every room where a work-related task has to be performed. This could remind the health care provider of all the tasks that are to be undertaken and will also help minimize errors or inefficiencies due to smartphone distraction and related multitasking.

3. Set up an intracompany social network that allows colleagues to communicate and exchange information in a secure fashion. This system would act as a substitute for the more popular and public social networks like Facebook and Twitter. Access to public social networks should then be restricted to the cellular/smartphone use zones.

4. Emphasize that voice-function capability be integrated into all health-related apps that might be used at the workplace.

5. Create a list of “high alert” or important phone numbers, messages, and emails. These numbers would be permitted to alert the professional during work. All other numbers would automatically go into “do not disturb” mode. Similarly, messages and emails that were not on the high-alert list would not alert the user. The cellular/smartphone use zones would allow professionals to handle non-work-related/non-urgent phone calls, messages, and emails.

6. Set up a combination of use-authentication techniques, which may include, but are not limited to, passwords, smart cards, and fingerprints.

7. Limit high-risk share interfaces like Bluetooth and Infrared.

8. Set up required security patches and permission to access company networks/intranets on personal devices.

9. Generate security alerts/warning messages if a compromised or unauthorized device is used on the network.

10. Generate security messages to the user who accesses unscrupulous or potentially unauthorized websites.

11. Establish strict regulations for taking pictures and videos via smartphones.

12. Provide health care professionals with periodic and relevant training in ethics and conflicts of interest, to help them decide if their actions would compromise the same.

Some of these solutions have already been deployed at various organizations.47,48

Similarly, taking into consideration that such devices can be a contamination risk, we recommend (1) the use of sterilized bags to store cellular/smartphones when entering patient-care and other sensitive zones, (2) the use of gloves while interacting with patient-care and other sensitive zones, (3) the use of new gloves after using a smart device in patient-care and other sensitive zones, and (4) the use of sanitizing wipes and/or hand sanitizers at regular intervals, especially before dealing with patients.

Based on the preceding discussion, a framework for smartphone use in health work settings was created. The framework illustrates various areas of concerns that need to be addressed by a smartphone usage policy aimed at minimizing distraction in a health care work setting. The framework is shown in Figure 1.

This framework is based on our current assessment. Future studies could focus on testing its validity. We feel that quantitative and/or quantitative methods could be employed to test this framework.

**Conclusion**

From the analysis above, it is clear that smart devices, including smartphones, form an integral part of our connected lives. However, they compromise security and privacy, quality of patient care, and efficiency, and are a source of distraction. The following set of best practices could serve as guidelines to alleviate the negative effects of smartphones in a health care workplace:

1. Store personal devices out of reach, and encourage the use of organization-provided devices that contain preinstalled job-specific functions and apps.

2. Create no-cellular/no-smartphone zones in sensitive areas like intensive care units (ICUs), operation theatres, and critical care units.
3. Regulate the kind of ring tones, alert tones, and other such sounds used by health care professionals on their phones at work.

4. Ensure that all digital data is appropriately encrypted, and that the network and devices associated with the network are password-protected.

5. Regulate access to social-networking sites like Facebook, Twitter, and YouTube, and promote an intracompany communication network in the workplace.


7. Create specific hotspots where personal devices may be used during breaks.

8. Promote hygienic use of devices in health care settings through the use of gloves and sanitizers.

9. Ensure that prior permission is obtained before taking photos and videos at work. While taking photos and videos, all must adhere to organizational ethics and conflict-of-interest policies.

10. Ensure high-security computing networks, with regulated use of outside devices.

The formulation of guidelines must not be limited to the list presented above. Guidelines must be adapted and must evolve in accordance with the changing technology and circumstances in which the technologies are being used. Nevertheless, a critical set of concerns must be addressed. The critical set of concerns is constituted by the causes of error and inefficiencies discussed in previous sections of this paper. These concerns and the associated objectives are presented in Table 4.

Health care organizations can regulate the use of smartphones while minimizing distractions by deploying effective and practical usage policies. Usage policies, if crafted well, can also be used to maximize work efficiency and facilitate improved communication and services. Last, each organization

Table 4 Critical concerns addressed by smartphone usage guideline

<table>
<thead>
<tr>
<th>Primary focus on patient-care</th>
<th>Safe and hygienic use</th>
<th>Legal compliance</th>
<th>Data security and access control</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Reduced distraction</td>
<td>• Reduced contamination risk from devices</td>
<td>• Polices for code of conduct and conflict of interest while using smartphones during patient-care</td>
<td>• Increased privacy</td>
</tr>
<tr>
<td>• Reduced errors and inefficiencies</td>
<td>• Recommended use of sanitary wipes and sanitizers</td>
<td>• Policies for taking pictures and videos during work related activities</td>
<td>• Regulate unauthorized access/use</td>
</tr>
<tr>
<td>• Regulated use of smartphones</td>
<td>• Recommended use of gloves, to be changed if smartphone is used</td>
<td>• Policies of sharing work related information on social networks</td>
<td>• Information security and regulated sharing of information</td>
</tr>
<tr>
<td>• Reduced contamination risk from devices</td>
<td>• Recommended use of sterilized pouches to store smart devices during patient-care</td>
<td>• Policies for use of smartphones during work</td>
<td>• Remote device management</td>
</tr>
<tr>
<td>• Improved patient privacy</td>
<td></td>
<td>• Review and update organization policies in timely manner and notify employees</td>
<td>• Theft prevention/counter measure (information and hardware)</td>
</tr>
<tr>
<td>• Improved patient satisfaction</td>
<td></td>
<td></td>
<td>• Improved user authentication</td>
</tr>
<tr>
<td>• Regulated use of the smartphone for emails, messages, Internet and apps during work</td>
<td></td>
<td></td>
<td>• Regulate high-risk sharing interfaces like Bluetooth and Infrared</td>
</tr>
<tr>
<td>Improved privacy management</td>
<td></td>
<td></td>
<td>• Block scrupulous or unauthorized websites/webpages</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Improved privacy management</th>
<th>Effective and efficient communication</th>
<th>Regulating cellular phone use zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Regulated smartphone use while at work</td>
<td>• Set up intra company communication channels</td>
<td>• Restrict use of smartphones in patient-care and sensitive zones</td>
</tr>
<tr>
<td>• Regulated access to the Internet and social networking/media sites</td>
<td>• Setup smartphone use zones, Wi-Fi hotspots</td>
<td>• Set up smartphone use zones, Wi-Fi hotspots</td>
</tr>
<tr>
<td>• Regulated sharing of information including photos and videos</td>
<td>• Setup ‘highalert’ lists of number, from whom calls, emails and messages are urgent and always permitted</td>
<td>• Set up smartphone use in cafes and break rooms</td>
</tr>
<tr>
<td>• Improved computing network and system privacy</td>
<td>• Voice capability function for work devices and health care related apps to minimize distraction while use</td>
<td>• Security patches and permission to access company networks/intranet on personal devices</td>
</tr>
<tr>
<td>• Improved user authentication</td>
<td></td>
<td>• Understanding that cellular phone use cannot be completely restricted</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Improved privacy management</th>
<th>Effective and efficient communication</th>
<th>Regulating cellular phone use zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Regulated smartphone use while at work</td>
<td>• Set up intra company communication channels</td>
<td>• Restrict use of smartphones in patient-care and sensitive zones</td>
</tr>
<tr>
<td>• Regulated access to the Internet and social networking/media sites</td>
<td>• Setup smartphone use zones, Wi-Fi hotspots</td>
<td>• Set up smartphone use zones, Wi-Fi hotspots</td>
</tr>
<tr>
<td>• Regulated sharing of information including photos and videos</td>
<td>• Setup ‘highalert’ lists of number, from whom calls, emails and messages are urgent and always permitted</td>
<td>• Set up smartphone use in cafes and break rooms</td>
</tr>
<tr>
<td>• Improved computing network and system privacy</td>
<td>• Voice capability function for work devices and health care related apps to minimize distraction while use</td>
<td>• Security patches and permission to access company networks/intranet on personal devices</td>
</tr>
<tr>
<td>• Improved user authentication</td>
<td></td>
<td>• Understanding that cellular phone use cannot be completely restricted</td>
</tr>
</tbody>
</table>
should consider its unique circumstances, and more importantly its mission and vision statements, when creating such policies.

Disclosure

The authors report no conflicts of interest in this work.

References


Risk Management and Healthcare Policy

Publish your work in this journal

Risk Management and Healthcare Policy is an international, peer-reviewed, open access journal focusing on all aspects of public health, policy, and preventative measures to promote good health and improve morbidity and mortality in the population. The journal welcomes submitted papers covering original research, basic science, clinical & epidemiological studies, reviews and evaluations, guidelines, expert opinion and commentary, case reports and extended reports. The manuscript management system is completely online and includes a very quick and fair peer-review system, which is all easy to use. Visit http://www.dovepress.com/testimonials.php to read real quotes from published authors.

Submit your manuscript here: http://www.dovepress.com/risk-management-and-healthcare-policy-journal