Approved October 10, 2015
Revised April 14, 2017

AST Guidelines for Best Practices in Use of Mobile Information Technology in the Operating Room

Introduction

The following Guidelines for Best Practices were researched and authored by the AST Education and Professional Standards Committee, and are AST approved.

AST developed the following guidelines to support healthcare delivery organizations (HDO) reinforce best practices in the use of mobile information technology (MIT) in the operating room (OR) as related to the role and duties of the Certified Surgical Technologist (CST®), the credential conferred by the National Board of Surgical Technology and Surgical Assisting. The purpose of the guidelines is to provide information OR supervisors, risk management, and surgical team members can use in the development and implementation of policies and procedures for the use of MIT in the surgery department. The guidelines are presented with the understanding that it is the responsibility of the HDO to develop, approve, and establish policies and procedures for the surgery department regarding the use of MIT according to established HDO protocols.

Rationale

Cell phones/smartphones, tablets, personal digital assistants (PDAs) and other mobile devices (referred to as "*mobile information technology [MIT]*) that can perform the functions of personal computers including taking photos, uploading and downloading files, instant access to and ability to quickly distribute information, and ability to record and transmit events as they are occurring has quickly become assimilated into medical practice. MIT is viewed by the medical community and patients as a primary source of communication and access to patient-related information.[1] HDOs, clinics, and physician' offices have devoted significant financial resources towards MIT to get the devices into the hands of medical staff for immediate access to patient data, drug information, case studies, surgeon's preference cards, and ability to quickly communicate among themselves.[2] Research studies have examined the influence of MIT on communication and team efficiency revealing the following advantages:

- Decrease in medical errors[3]
- Faster access to patient information[4,5,6,7,8]
- Improved communication with patients[7,8]
- Improved work productivity and efficiency[9,10]
- Preoperatively distracting pediatric patients[7]
- Decrease in failure-to-respond rate as compared to the use of pagers[9,10,11,12,13]

However, technology comes with challenges and in this instance a key challenge is monitoring the appropriate use of MIT in the OR (and other critical care areas of the HDO). The problem has been referred to as "*distracted doctoring*" in which healthcare personnel (HCP) are focused on the screen and not the patient including conducting personal business and accessing Internet sites during surgical procedures, in the ICU, and other critical care units.[2,14] For example, medical students and residents are under increasing pressure to access MIT such as iPads and smartphones that are being provided to them by the school; the pressure originates from the drive in modern medicine that patient care is data driven and immediate access to the latest information is a priority. The American Association of Nurse Anesthetists summed up the issue in their position statement by stating "non-essential distractions, especially those associated with the use of mobile information technology (e.g., smartphones, tablets, personal digital assistants [PDAs]), the Internet, and the data accessed through these tools, may lead to significant patient safety lapses."[15] OR personnel preoccupied by a mobile device including texting, accessing social networks, reading or using mobile devices on a general non-clinical basis is distracted from the primary task and therefore, considered a patient safety issue.[15,16,17]

In response, HDOs have begun establishing policies and procedures that limit the use of MIT in critical care settings, and some medical schools have started reminding students and residents to focus on the patient and use the mobile device at the appropriate time.[2] As Dr. Peter W. Carmel, President of the American Medical Association has said, technology "offers great potential in health care", but the doctors' first priority should be with the patient.[2] This should also be the priority of CSTs while providing perioperative care to the surgical patient, and not allow mobile devices to come between them and the patient.

Evidence-based Research and Key Terms

The research of articles, letters, nonrandomized trials, and randomized prospective studies was conducted using the Cochrane Database of Systematic Reviews and MEDLINE®, the U.S. National Library of Medicine® database of indexed citations and abstracts to medical and healthcare journal articles.

The key terms used for the research of the Guidelines include: auto-location technology; cross-contamination; distracted doctoring; electromagnetic interference; mobile information technology; non-critical care areas; protected health information; social media. Key terms used in the Guidelines are italicized and included in the glossary.

Guideline I

Mobile devices must be properly cleaned and disinfected prior to being brought into the surgery department or other critical care unit, e.g. preoperative holding or PACU.

1. Mobile devices are a source of *cross-contamination* and can contribute to microbial contamination in the OR.
    A. In the U.S., 1.7 million patients are affected by healthcare-associated infections (HAI).[18] Multiple studies have confirmed that over 90% of HCPs' cell phones tested positive for bacteria, including methicillin-resistant *Staphylococcus aureus* (MRSA) and other microbes that can cause HAIs.[19,21,22,23,24]
    B. Jeske et al. reported that even after 40 anesthesia care providers used hand sanitizer, the majority of mobile devices were found to have pathogens.[24]

C. A clinical microbiological study completed in 2011 revealed that more than 84% of cultures obtained from swabbing cell phones were positive for microbial contamination including *Staphylococcus aureus* and MRSA.[25]

2. Devices should be properly cleaned and disinfected on a routine basis, and before entering the surgery department or other patient care area, eg, preoperative holding and PACU.
    A. Mobile devices as well as the OR computers should be routinely cleaned with a manufacturer-approved antimicrobial wipe to avoid damaging the display screen and to reduce the potential for cross-contamination.[8,26,27,28]
        1) Some literature suggests using alcohol wipes to disinfect mobile devices; however, care must be taken to not use products that degrade the display screen.[27] For example, Apple recommends that alcohol and ammonia should not be used on iPads or iPhones.[29]
    B. OR personnel should practice strict hand hygiene before and after the use of a mobile device, particularly if he/she will be providing patient care.[23,28,30]
3. HDO policies should include addressing the cleaning and disinfection of mobile devices and computers for OR personnel to strictly follow.
    A. The HDO should provide continuing education on the ways that mobile devices can carry and transmit pathogens, preventive measures for decontaminating the devices as developed by the HDO's infection control committee, and other measures that prevent cross-contamination when providing patient care.[8]

Guideline II

Personal mobile devices should only be used in HDO designated *non-critical care areas* by OR personnel.

1. HDOs should establish zones or areas with Wi-Fi hotspots for the use of mobile devices for personal or non-critical care reasons, e.g., CST who works for a surgeon group practice contacts the clinic to have the next day's schedule sent to his/her smartphone.[16] It is recommended the zones are integrated with cafes or department break rooms to ensure OR personnel are separated from work-related activities.[16]
    A. Research on the subject of unsafe practices and risks to patient care caused by the use of mobile devices supports HDO policies regarding controlling their use.[31]
        1) In the September 2011 edition of the journal *Perfusion* the results of a survey on cell phone use by perfusion technicians while administering cardiopulmonary bypass (CPB) were published. Of the 439 clinical perfusion technicians who completed the survey, 55.6% reported talking on a cell phone during surgery and 49.2% reported texting during surgery. Regarding smartphone use, 21% accessed E-mails; 15.1% accessed the Internet, 3.1% checked and/or posted on social networking sites.[32]

            The article also reported that 7.3% of the technicians admitted that personal distraction by cell phone use negatively affected their performance and 33.7% of the technicians reported

seeing another perfusionist distracted by cell phone use or texting during surgery. However, 78.3% expressed the opinion that cell phone distraction can be a potentially significant safety risk to patients.[32]

B. OR personnel should never access a cell phone either directly or using a wireless headset during perioperative care of the patient.[31] Additionally, OR personnel should never use the OR computer for personal use, e.g., browsing through Internet sites, checking and/or posting on social networking sites. The activities of OR personnel should be solely focused on the perioperative care of the patient in order to avoid medical errors.[33] OR personnel who are focused on a device's screen rather than focused on the patient may miss indications of the patient's condition and/or indications of an impending medical emergency, e.g. cardiac arrest during surgery.
    1) The following serves as an example of the level of safety risk a patient is placed when OR personnel are not focused on the procedure. The *New York Times* published a report of a neurosurgeon who was distracted during an operation while making personal phone calls using a wireless headset and the patient was left partially paralyzed.[2]
    2) Dr. John Halamka wrote up a case study that illustrates how distractions by mobile devices place patients at risk and further emphasizes that the patient should be the center of attention. A resident physician was using a smartphone to enter an order to stop anticoagulation therapy for a patient in the HDO's EHR system as ordered by the attending physician. Before completing the order the resident received a personal text message about a party that was soon to be held. The resident responded to the text message, but never resumed finishing the patient order. The patient continued to receive anticoagulation therapy for several days resulting in conditions that required emergency open-heart surgery.[34]
    3) A recommendation is for the HDO in conjunction with the information technology department to create a priority list of phone numbers and/or email addresses that would be allowed to alert the user during work. All other numbers and email addresses not on the priority list would automatically enter the "do not disturb" mode.[16]

C. The ring tone of mobile devices can be a source for interrupting the care of the surgical patient.
    1) The ring tone of a cell phone, or noticeable vibration, can disrupt the communication of the team in the OR. Alarm tones on medical equipment may be overlooked by the OR team if confused with cell phone ring tones.
    2) The OR team should remember the strongest sense that the patient experiences in the OR is hearing, in particular just prior to general anesthesia taking full effect or if the procedure is performed under local sedation. The patient may be startled and experience unnecessary anxiety by a ring tone or vibration.

D. Smartphones are limited by the small screen that may not properly and clearly display information that can be a patient safety risk. For example an electronic health record (EHR) system that is designed for use on a laptop or desktop computer may be displayed poorly on the small screen of the smartphone. Additionally, the user may need to scroll through the information possibly missing vital patient information that is hidden from view on the smaller screen.[35]

E. OR personnel should avoid sending job-related messages to other HDO departments or clinicians by text messaging.[31]

1) Many clinicians who use smartphones to send job-related messages do so by text messages.[8] Texting has limitations that make it inappropriate for communications related to patient care. In 2011, the Joint Commission issued the following statement:

> This method provides no ability to verify the identity of the person sending the text and there is no way to keep the original message as validation of what is entered into the medical record.[36]

Guideline III

OR personnel should turn off mobile devices in the presence of critical care or life support medical equipment to prevent interference with the functioning of the equipment.

1. Controversy exists as to the extent of mobile devices *electromagnetic interference* (EMI) with medical equipment.[8,37] There is concern that the newer generation of mobile devices that can access the Internet as well as receive and send information may increase the incidences of EMI.[38] Regardless of the improved magnetic shielding of critical care and life support equipment, there is a possibility that EMI can cause equipment to either display an incorrect value, or alter the baseline movements or information causing the alarm to activate.
    A. Studies have reported contradictory results regarding EMI due to the use of mobile devices.
        1) A 2005 study reported a 1.2% incidence of interference out of 500 tests and concluded there was clinically significant interference.[39]
        2) Incidences of medical devices, such as infusion pumps and ventilators, affected by EMI have been reported as well as anesthesia care providers reporting interference with anesthesia equipment by cell phones.[8,40]
        3) A study reported a controlled laboratory test of 76 types of OR and ICU equipment that 15% of the equipment was affected by mobile device signals.[37]
2. The effect and degree of EMI depends on the type of mobile device and power output, susceptibility of the medical device to EMI, and distance between the mobile and medical device.[8,37]
    A. The higher the output power of a mobile device the higher the risk of EMI.[8] A Wi-Fi connection has much lower power than a cellular connection, thus less likely to cause EMI.[8] Wi-Fi connections are consistently safely used in HDOs, including near medical equipment. OR personnel should configure

their smartphone to use a Wi-Fi connection when accessing the Internet to reduce the risk of EMI. However, the risk for EMI is not eliminated because the smartphone will still use a cellular service for phone calls.[8]

B. OR personnel should follow the equipment manufacturer's recommendations regarding the distance between the equipment and use of mobile devices to avoid EMI. The surgery department should also consult with the biomedical engineering department for assistance in completing a patient risk analysis of existing and new equipment.

C. HDOs should establish policies that address limiting the use of mobile devices by HCP in the specific areas of the HDO where critical care and life support equipment is being used.

    1) It is recommended that mobile devices should be used at a minimum of 1 meter (approximately 3 feet) away from medical equipment to prevent EMI.[8,9,13,38,41-44]

D. Patients and visitors should be informed that the use of mobile devices near medical devices can disrupt the medical devices functionality placing the patient at risk.

    1) Patients and visitors should be prohibited from using mobile devices in critical care areas where multiple medical devices are in use. The areas should be indicated by easily noticeable signage. The mobile device must be powered off when carried into these areas.
    2) However, the facility needs to be sensitive to the need for visitors to communicate with others outside the HDO from areas such as the surgical waiting room or emergency department. The visitor(s) should be instructed to use the mobile devices at least 1 meter or more away from medical equipment. If not possible to maintain the distance, the visitor should be instructed not to use the mobile device.
    3) The same applies to patients; if the patient is undergoing treatment in which medical equipment is being used, the patient should be instructed not to use a mobile device since a 1 meter distance cannot be maintained.

Guideline IV

OR personnel have the duty to responsibly use MIT without violating patient confidentiality, *protected health information* (PHI), and state and federal patient privacy laws.

1. HDOs and OR personnel are responsible for the security of patient confidentiality, data, information, and privacy.[45]

    A. Mobile devices that have photo and/or video capturing capabilities should not be used in the presence of surgical patients throughout the perioperative course of treatment. The use of mobile devices in this manner can lead to compromising patient confidentiality and privacy, as well as violate patient privacy laws. OR personnel and HDOs are referred to the ECRI March 2012 report *Photography, Filming and other Imaging of Patients* published in *Healthcare Risk Control* for details regarding the inappropriate use of

mobile device cameras as well as recommendations for photo-taking policies that protect the privacy of PHI, patients, and staff. The following are general recommendations.

1) The Health Insurance Portability and Accountability Act (HIPAA) *Standards for Privacy of Individually Identifiable Health Information*, commonly referred to as the Privacy Rule, protects all individually identifiable health information held or transmitted in any form or media. Individually identifiable health information is defined as past, present, or future physical or mental health information that may allow another person to identify an individual including name, address, Social Security number and demographic information.[8,45]
2) OR personnel should not post PHI, videos or photographs of surgical patients on blogs, discussion boards, or *social media* sites. Additionally, the information should not be shared through email or texting.
3) Violations of patient confidentiality can result in severe consequences including loss of job, removal of certification or licensure, and legal actions.[39,45,46] In 2010 the National Council of State Boards of Nursing completed a survey of state's Board of Nursing (BON). 33 of the 46 BONs that responded reported receiving complaints of RNs who violated patient privacy by posting patient information and photos on social media sites. 26 of the 33 BONs reported undertaking disciplinary action as a consequence of the complaints.[47]
4) HDOs should develop and periodically review policies that address photography, filming, video capturing and other types of imaging.
    a) The policies should address use by medical staff, employees, patients, visitors and volunteers. The HDO should anticipate all instances of how cameras could be used, e.g., patient or visitor taking personal photographs; medical staff, employee, or student taking photos of patient care and/or treatment; telemedicine; marketing photos of HDO.[8]
    b) The policies should address the various types of devices that have photographic capturing capabilities, eg, wireless handheld devices; webcams on laptop computers.[8]
    c) The policies should prohibit employees, medical staff and volunteer from using their own mobile device or a facility-supplied device to take photographs or videos of patients and visitors that are not related to the patient's care, eg personal reasons.[8]
    d) The policies should establish the specific circumstances in which a surgeon should obtain the patient's written consent to take photographs or other images related to treatment and how the media will be used. HIPAA authorization is not required for taking treatment-related images, but obtaining

the patient's permission is in the interests of upholding risk management best practices.[8] The policy should specify that OR personnel and/or surgeon must use mobile devices provided or approved by the HDO, and security measures must be established to prevent access to and inappropriate use of the images by outsiders.

e) Establish policies that safeguard the storage of photographs and other images in the patient's medical record since these are considered PHI.

B. PHI should only be saved on HDO-approved, secure file servers or encrypted devices. OR personnel should access the information only through facility-approved methods.[16,48] HDOs have multiple options available to assist in protecting PHI, but still allow OR personnel the ability to access information that is critical to patient care.

1) HDO provides organization-owned smartphones and other mobile devices: This provides the HDO greatest control of PHI; information technology (IT) personnel can control the applications that are loaded on the devices and ensure the most current security software and malware is loaded, and kept up-to-date.[16]
2) OR personnel' personal device is cleared for use by the HDO: An HDO only allows the use of personal devices that meet the HDO's security requirements to access the facility's system.[8,16]
3) Access information on HDO server: OR personnel use their personal device to log-in and access information stored on the facility's server, but the information is not stored on the device. This option reduces security risks if the device is lost, stolen, or compromised by an outside source, e.g. "hacking".
4) HDO requires a user agreement: HDO requires OR personnel to sign an agreement that their personal mobile devices must meet the same security measures as the facility's internal devices and servers.[8] The user has access to the facility's server, but if the device is stolen, lost or compromised agrees that the facility has the right to remotely wipe data from the device which means the user's personal data will also be deleted.
5) Separation or segregating of data: Software is available that keeps the HDO's data separate from the user's personal information. This allows the facility's information to be wiped from the device, but preserves the user's personal information in the event the device is lost.[35]
6) HDO's should have a policy addressing if a user changes or upgrades their smartphone or other mobile device. The user should provide the old device to the IT department to scan and wipe out any PHI and facility information prior to donating or disposing the device.[8]

C. The Healthcare Information and Management Systems Society (HIMSS) Mobile Security Work Group published a report on security threats addressing the possibility of someone eventually developing malware to compromise patient data on mobile devices.[49] The following are recommendations for protecting the security of OR personnel smartphone use.[50]
    1) OR personnel should ensure that their smartphones include security controls that are routinely updated with the most recent antivirus software and malware protection.[8,16]
    2) Password protection should be used in order for an individual to unlock a mobile device and possibly prevent a security breach if a device is lost or stolen. The Internet security software business Symantec conducted an experiment in which employees intentionally "lost" 50 phones. The business observed the majority of individuals who found phones tried to access the device before returning.[16,51]
    3) *Auto-location technology*, such as GPS functionality, should be loaded onto mobile devices to assist the user and/or HDO locate a lost or stolen device.[16,35]
    4) PHI files and other sensitive HDO information stored on mobile devices should also be password protected to prevent access.
    5) The device should be programmed to lock-up after a specific number of attempts by a user to log-on, e.g. incorrect password.
    6) Automatic log-off should be loaded onto mobile devices activated by the device after a specific period of time of being idle.[8]
    7) HDO sets up a system where a security alert/warning message is sent to all healthcare personnel within the facility that a compromised or unauthorized device is being or has been used on the network.[16] This allows personnel to stop using their mobile device until the situation has been resolved.
    8) HDO sets up a system where a user who accesses an unauthorized website receives a security alert/warning message.[16]

2. HDOs should establish policies that reinforce the protection of patient privacy as well as strengthen patient care by prohibiting the inappropriate use of MIT and OR computers during perioperative care of the surgical patient. The policies need to ensure that any kind of personal interruptions by mobile devices is avoided when patient care is being provided.[16,50]
    A. The policies should address appropriate and inappropriate use of mobile devices when providing patient care, areas or zones within the HDO where non-clinical use of mobile devices is allowed, use of social media, and use of encrypted devices to securely access patient information and data.[15] The policy should also address in detail the consequences for violations including violation of patient confidentiality and privacy.

B. CSTs should always comply with HDO policies regarding the use of mobile devices. By remaining focused on the patient, a CST can reduce distractions, errors, and inefficiencies when adhering to the MIT policy of the employer. Regulated use of mobile devices improves management of data security, patient privacy and patient satisfaction.

3. HDOs should establish policies addressing the use of mobile devices by patients and their family and friends in order to protect the privacy of other patients.
   A. Patients, family and friends may want to take photos or video recordings of their visits at the HDO. However, patients often share rooms and the photo or video recordings could inadvertently include images of the patient who is not part of the visitation. Additionally, images of patients in the hallway could unintentionally, be included in the photos or video recordings.
   B. The HDO will need to decide if it will allow the use of mobile devices inside the facility by patients and visitors.[50]
      1) Due to the challenge it would present to HCP in monitoring the use of mobile devices, it is recommended that HDOs create a policy that prohibits the use of mobile devices by patients and visitors while inside the HDO.
      2) Upon admission, the HDO should have the patient sign and date a copy of the policy that is kept in the patient's file in addition to informing the patient through the HDO's HIPAA privacy notice.[8] Visitors should also be provided the written picture-taking policy. The policy should inform the patient and visitors that the facility has the right to delete images that were acquired without the appropriate consent or permission.
      3) The HDO should display signage with information about the policy throughout the facility. The display should include a graphic symbol such as an 'X' over the drawing of a person talking on a cell phone and/or taking a photo.
      4) If the facility allows photos to be taken patients and visitors will need to be educated about the privacy issues of other patients and employees. The facility policy should require the patient and/or visitor to obtain the permission of another patient, employee, medical staff, or volunteer who may appear in the photograph in order to respect the privacy of others.[8] Individuals must be prohibited from taking photographs that include medical devices that display patient data.
      5) The policy should authorize HDO staff to address patients and visitors using mobile devices while inside the facility.

Guideline V

OR personnel should use email and smartphones in an efficient and professional manner to coordinate the effective care of surgical patients.

1. Studies have identified both positive and negative outcomes with the use of smartphones between physicians, allied health professionals and nurses.
    A. There is a perceived improvement in the efficiency of using smartphones and email over the use of pagers.[40,52]
        1) Allied health professionals and nurses found that when faced with an urgent patient care issue being able to directly call a resident or physician eliminated the need to wait for a telephone call reply to the page, which also decreased the occurrence of "phone tag".[53]
        2) Equally, non-urgent issues can be efficiently communicated by allied health professionals and nurses through the use of email to prevent disrupting the resident or physician.[54,55]
    B. Results of studies have identified professional issues associated with the use of smartphones that healthcare personnel (HCP) should immediately resolve to achieve a positive outcome for the patient.
        1) Interviews with staff physicians and residents identified a perceived increase in the number of calls and messages received causing interruptions in patient care and teaching.[56,57] Physicians have observed these interruptions could have negative impacts on the communication and interaction with patients including adverse events.[53]
        2) There is a "gap in perceived urgency" meaning what the allied health professional or nurse considers an urgent patient issue as opposed to the physician or resident not considering urgent, thus not responding or delaying a response to the email or smartphone message.[53,55,58] Rather than allowing the issue to become a significant barrier to providing quality patient care, the healthcare team should address the issues including establishing parameters as to when and how physicians and residents should be contacted, e.g. abnormal vital signs in preoperative holding or PACU, abnormal bleeding in PACU.
        3) All HCP, including physicians, residents, allied health professionals, and nurses, should be aware of instances when interrupting conversations or professional rounds by answering a smartphone or email message could be regarded as disruptive, especially when discussing the details of a patient, and unprofessional.[59,60,61] Additionally, this behavior could be a source for creating a negative perception among patients and if they are receiving the full attention of the HCP.[54]

Guideline VI

CSTs should complete continuing education regarding HIPAA regulations and the risks associated with the use of mobile devices.

1. Surgery departments should provide annual continuing education for OR personnel to complete regarding the review of HIPAA regulations and the Privacy Rule to ensure that they are strictly adhered to on a daily basis.
    A. The continuing education should include the appropriate use of MIT, social media, and OR computers as well as patient privacy and PHI policies.
        1) The surgery department should document the completion of the continuing education in the file of each OR personnel.
2. Surgery departments should provide annual continuing education for OR personnel regarding unsafe practices that could introduce malware into a mobile device and OR computer that could compromise patient data, eg opening suspicious attachments or clicking on unreliable Internet links.
3. The continuing education should be based upon the concepts of adult learning, referred to as andragogy. Adults learn best when the information is relevant to their work experience; the information is practical, rather than academic; and the learner is actively involved in the learning process.[64]
4. It is recommended surgery departments use various methods of instruction to facilitate the learning process of CSTs
    A. If the education is primarily lecture, methods to engage learners include presentation of case studies for discussion, and audience discussion providing suggestions for reinforcing the proper use of MIT.
    B. Other proven educational methods include interactive training videos, and computerized training modules and teleconferences.
    C. The continuing education should be delivered over short periods of time, such as in modules, and not in a one-time lengthy educational session.
5. Continuing education programs should be periodically evaluated for effectiveness including receiving feedback from surgery department personnel.
6. The surgery department should maintain education records for a minimum of three years that include dates of continuing education; names and job titles of employees that completed the continuing education; synopsis of each continuing education session provided; names, credentials, and experience of instructors.

Competency Statements

Competency Statements	Measurable Criteria
1. CSTs have the knowledge and ability to apply professional ethics in safeguarding PHI and the privacy of patients. 2. CSTs demonstrate surgical conscience and professional ethics regarding the uninterrupted care of surgical patients. 3. CSTs have knowledge of the principles of asepsis and their application to the use of mobile devices and patient care. 4. CSTs can serve on as well as participate in the work of a mobile information technology HDO committee that is charged with establishing and overseeing policies that address the use of mobile devices within the facility.	1. Educational standards established by the *Core Curriculum for Surgical Technology*.[62] 2. The didactic subject of surgical conscience and professional ethics in the OR is included in a CAAHEP accredited surgical technology program. 3. The didactic subject of principles of asepsis is included in a CAAHEP accredited surgical technology program. 4. Students demonstrate knowledge of surgical conscience, professional ethics and principles of asepsis in the lab/mock OR and during clinical rotation. 5. CSTs work with surgical team to ensure the privacy and confidentiality of surgical patients including PHI. 6. CSTs practice principles of asepsis daily in the OR and during other related patient care activities to prevent cross-contamination. 7. CSTs participate on HDO committees including a mobile information technology committee. 8. CSTs complete continuing education to remain current in their knowledge of legal issues, risk management, professional ethics, surgical conscience and sterile technique.[63]

CST® is a registered trademark of the National Board of Surgical Technology and Surgical Assisting (NBSTSA).

Glossary

Auto-location technology: Software loaded onto a mobile device that uses Global Positioning System (GPS) to enable an individual to remotely track a lost or stolen device.

Cross-contamination: Unintentional transfer of microbes from HCP to patient or vice versa, or fomite to patient or HCP.

Distracted doctoring: Term used to describe when HCP are preoccupied by mobile information technology, such as cell phones, rather than focusing on the patient.

Electromagnetic interference: Disturbance caused by an external source, such as a cell phone, that affects electrical circuits.

Mobile information technology: Term used to describe electronic devices that can be easily transported or carried by the user, including cell phones and tablets.

Non-critical care areas: Term used to describe areas where patient care is not delivered including break rooms, cafeteria, and locker/changing room.

Protected health information: Any information or data collected by HCP about a patient that is confidential including demographic information, health record, insurance information, laboratory results, and medical history.

Social media: Web sites and applications that allow users to create and share content or participate in social networking.

References

1. Katz, JD. Noise in the operating room. *Anesthesiology*. Oct. 2014; 121(4): 894-898.
2. Richtel, M. As doctors use more devices, potential for distraction grows. *The New York Times*. Dec. 14, 2011; http://www.nytimes.com/2011/12/15/health/as-doctors-use-more-devices-potential-for-distraction-grows.html?pagewanted=all. Accessed June 30, 2015.
3. Prgomet M, Georgiou A., Westbrook JI. The impact of mobile handheld technology on hospital physicians' work practices and patient care: a systematic review. *J Am Med Inform Assoc*. Nov-Dec 2009; 16(6): 792-801
4. Dasari KB, White SM, Pateman J. Survey of iPhone usage among anaesthetists in England. *Anaesthesia*. Jul 2011; 66(7): 630-631.
5. Bhansali R, Armstrong J. Smartphone applications for pediatric anesthesia. *Paediatr Anaesth*. Apr 2012; 22(4): 400-404.
6. Dala-Ali BM, Lloyd MA, Al-Abed Y. The uses of the iPhone for surgeons. *Surgeon*. Feb 2011; 9(1): 44-48.

7. Gapinski K. 7 Ways to use smartphones and tablets in the OR. *Outpatient Surgery*. October 2014; 25(10).
8. ECRI Institute. Judgment call: smartphone use in hospitals requires smart policies. *Health Devices*. Oct 2012; 41(10): 314-329.
9. Ruskin KJ. Communication devices in the operating room. *Curr Opin Anaesthesiol*. Dec 2006; 19(6): 655-659.
10. Wu R, Rossos P, Quan S, Reeves S, Lo V, Wong B, Cheung M, Morra D. An evaluation of the use of smartphones to communicate between clinicians: a mixed-methods study. *J Med Internet Res.* 2011; 13(3):e59.
11. Aziz O, Panesar SS, Netuveli G, Paraskeva P, Sheikh A, Darzi A. Handheld computers and the 21st century surgical team: a pilot study. *BMC Med Inform Decis Mak.* 2005;5:28.
12. Richardson JE, Shah-Hosseini S, Fiadjoe JE, Ash JS, Rehman MA. The effects of a hands-free communication device system in a surgical suite. *J AM Med Inform Assoc*. Jan-Feb 2011; 18(1): 70-72.
13. Soueid A. A new tool for the operating surgeon: a Bluetooth mobile phone headset. *Burns*. Nov 2006; 32(7): 927-928.
14. Gold J. Hospitals warn smartphones could distract doctors. *NPR*. March 26, 2012; http://www.npr.org/2012/03/26/149376254/hospitals-guard-against-smartphones-distracting-doctors. Accessed June 30, 2015.
15. American Association of Nurse Anesthetists. Mobile information technology: position statement. *AANA*. Feb 2015; http://www.aana.com/resources2/professionalpractice/Documents/Mobile%20Information%20Technology.pdf. Accessed June 30, 2015.
16. Preetinder SG, Kamath A, Gill TS. Distraction: an assessment of smartphone usage in health care work settings. *Risk Manag Healthc Policy*. 2012; 5: 105-114.
17. Shelton JT, Elliott EM, Lynn SD, Exner AL. The distracting effects of a ringing cell phone: an investigation of the laboratory and the classroom setting. *J Environ Psychol*. Dec 2009; 29(4): 513-521.
18. Manning ML, Davis J, Sparnon E, Ballard RM. iPads, droids, and bugs: infection prevention for mobile handheld devices at the point of care. *Am J Infect Control*. Nov 2013; 41(11): 1073-1076.
19. Brady RR, Fraser SF, Dunlop MG, Paterson-Brown S, Gibb AP. Bacterial contamination of mobile communication devices in the operative environment. *J Hosp Infect*. 2007: 66(4): 397-398.
20. Hassoun A, Vellozzi EM, Smith MA. Colonization of personal digital assistants carried by healthcare professionals.
21. Braddy CM, Blair JE. Colonization of personal digital assistants used in a health care setting. *Am J Infect Control*. May 2005; 33(4): 230-232.
22. Al-Abdalall AH. Isolation and identification of microbes associated with mobile phones in Dammam in eastern Saudi Arabia. *J Family Community Med*. Jan 2010; 17(1): 11-14.
23. Ustun C, Cihangiroglu M. Health care workers' mobile phones: a potential cause of microbial cross-contamination between hospitals and community. *J Occup Environ Hyg*. 2012; 9(9): 538-542.

24. Jeske HC, Tiefenthaler W, Hohlrieder M, Hinterberger G, Benzer A. Bacterial contamination of anaesthetists' hands by personal mobile phone and fixed phone use in the operating theatre. *Anaesthesia*. Sep 2007; 62(9): 904-906.
25. Brady RR, Hunt AC, Visvanathan A, Rodrigues MA, Graham C, Rae C, Kalima P, Paterson HM, Gibb AP. Mobile phone technology and hospitalized patients: a cross-sectional surveillance study of bacterial colonization, and patient opinions and behaviors. *Clin Microbiol Infect*. Jun 2011; 17(6): 830-835.
26. Beer D, Vandermeer B, Brosnikoff C, Shokoples S, Rennie R, Forgie S. Bacterial contamination of health care workers' pagers and the efficacy of various disinfecting agents. *Pediatr Infect Dis J*. Nov 2006; 25(11): 1074-1075.
27. Visvanathan A, Gibb AP, Brady RR. Increasing clinical presence of mobile communication technology: avoiding the pitfalls. *Telemed J E Health*. Oct 2011; 17(8): 656-661.
28. Brady RR, Chitnis S, Stewart RW, Graham C, Yalamarthi S, Morris K, NHS connecting for health: healthcare professionals, mobile technology, and infection control. *Telemed J E Health*. May 2012; 18(4): 289-291.
29. Apple, Inc. Cleaning your Apple products. July 29, 2015; https://support.apple.com/en-us/ht204172. Accessed August 15, 2015.
30. Association of Surgical Technologists. Standards of practice for surgical attire, surgical scrub, hand hygiene and hand washing. April 13, 2008. http://www.ast.org/uploadedFiles/Main_Site/Content/About_Us/Standard_Surgical_Attire_Surgical__Scrub.pdf. Accessed June 30, 2015.
31. Luthra S. Do cell phones belong in the operating room? *PBS Newshour*. July 15, 2015; http://www.pbs.org/newshour/rundown/cell-phones-belong-operating-room/. Accessed August 15, 2015.
32. Smith T, Darling E, Searles B. Survey on cell phone use while performing cardiopulmonary bypass. *Perfusion*. May 2011; 26(5): 375-380.
33. Ettelt S, Nolte E, McKee M, Haugen OA, Karlberg I, Klazinga N, Ricciardi W, Teperi J. Evidence-based policy? The use of mobile phones in hospital. Dec 2006; 28(4): 299-303.
34. Halamka J. Order interrupted by text: Multitasking mishap. *AHRQ*. Dec 2011; http://webmm.ahrq.gov/case.aspx?caseID=257. Accessed June 30, 2015.
35. Cerrato P. Why BYOD doesn't always work in healthcare. *InformationWeek*. Feb 2012; http://www.informationweek.com/news/healthcare/security-privacy/232601666. Accessed June 30, 2015.
36. Joint Commission. Texting orders. *Standards FAQ Details*. Apr 2015; http://www.jointcommission.org/standards_information/jcfaqdetails.aspx?StandardsFaqId=658&ProgramId=47. Accessed June 30, 2015.
37. Mahmoud PA, Aghajani M, Nabipour I, Assadi M. An update on mobile phones interference with medical devices. *Radiat Prot Dosimetry*. Oct 2013; 156(4): 401-406.
38. van Lieshout EJ, van der Veer SN, Hensbroek R, Korevaar JC, Vroom MB, Shultz MJ. Interference by new-generation mobile phones on critical care medical equipment. *Crit Care*. 2007: 11(5): R98.
39. Abenstein JP. Safety while swimming in a sea of energy. *Mayo Clin Proc*. Mar 2007; 82(3): 276-278.

40. Soto RG, Chu LF, Goldman JM, Rampil IF, Ruskin KJ. Communication in critical care environments: mobile telephones improve patient care. *Anesth Analg*. Feb 2006; 102(2): 535-541.
41. Wallin MK, Marve T, Hakansson PK. Modern wireless telecommunication technologies and their electromagnetic compatibility with life-supporting equipment. *Anesth Analg*. Nov 2005; 101(5): 1393-1400.
42. Mobile phones and hospital equipment. *Evid Based Healthc Public Health*. April 2005: 9(2): 173.
43. Datta R. Mobile phones – ban or boon? *Med J Armed Forces India*. 2008; 64(4): 363-364.
44. Small D. Mobile phones should not be used in clinical areas or within a metre of medical equipment in hospitals. *Evid Based Healthc Public Health*. April 2005; 9(2) 114-116.
45. US Department of Health & Human Services. Health information privacy: All case examples. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html. Accessed June 30, 2015.
46. Lambert KM, Barry P, Stokes G. Risk management and legal issues with the use of social media in the healthcare setting. *J Healthc Risk Manag*. 2012; 3(4): 41-47.
47. National Council of State Boards of Nursing. A nurse's guide to the use of social media. Nov 2011. https://www.ncsbn.org/NCSBN_SocialMedia.pdf. Accessed June 30, 2015.
48. Kavoussi SC, Huang JJ, Tsai JC, Kempton JE. HIPAA for physicians in the information age. *Conn Med*. Aug 2014; 78(7): 425-427.
49. Healthcare Information and Management Systems Society. Security of mobile computing devices in the healthcare environment. *HIMSS Mobile Security Work Group*. Nov 2011; http://s3.anazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/PrivacySecurity/HIMSS_Mobility_Security_in_Healthcare_Final.pdf. Accessed June 30, 2015.
50. Warwick A. How to write a smartphone policy: Warwick Ashford outlines the factors CIOs must consider in writing policy for employees using smartphones for work. *Computer Weekly*. Feb 2012; http://business.highbeam.com/411267/article-1G1-283834925/write-smartphone-policy-warwick-ashford-outlines-factors. Accessed June 30, 2015.
51. Dolan PL, How to ensure a lost mobile device won't cause a data breach. *American Medical News*. Mar 2012; http://www.amednews.com/article/20120326/business/303269975/5/. Accessed June 30, 2015.
52. Coiera E. When conversation is better than computation. *J Am Med Inform Assoc*. May-Jun 2000; 7(3): 277-286.
53. Wu R, Rossos P, Quan S, Reeves S, Lo V, Wong B, Cheung M, Morna D. An evaluation of the use of smartphones to communicate between clinicians: a mixed-methods study. *J Med Internet Res*. Jul-Sep 2011; 13(3): e59.
54. Rivera-Rodriguez AJ, Karsh BT. Interruptions and distractions in healthcare: review and reappraisal. *Qual Saf Health Care*. Aug 2010; 19(4): 304-312.

55. O'Connor C, Friedrich JO, Scales DC, Adhikari NK, The use of wireless e-mail to improve healthcare team communication. *J Am Med Inform Assoc*. Sep-Oct 2009; 16(5): 705-713.
56. Collins S, Currie L, Bakken S, Cimino JJ. Interruptions during the use of a CPOE system for MICU rounds. *AMIA Annu Symp Proc*. 2006: 895.
57. Brixey JJ, Tang Z, Robinson DJ, Johnson CW, Johnson TR, Turley JP, Patel VL, Zhang J. Interruptions in a level one trauma center: a case study. *Int J Med Inform*. Apr 2008; 77(4): 235-241.
58. Hickam DH, Severance S, Feldstein A, Ray L, Gorman P, Schuldheis S, Hersh WR, Krages KP, Helfand M. The effect of health care working conditions on patient safety. *Evid Rep Technol Assess (Summ)*. Mar 2003; (74): 1-3.
59. Parikh SM, Liu E, White CB. Connectivity need not come at the expense of professionalism. *Acad Med*. Jun 2010; 85(6): 930.
60. Swick HM. Toward a normative definition of medical professionalism. *Acad Med*. Jun 2000; 75(6): 612-616.
61. ABIM Foundation, American Board of Internal Medicine, ACP-ASIM Foundation, American College of Physicians – American Society of Internal Medicine, European Federation of Internal Medicine. Medical professionalism in the new millennium: a physican charter. *Ann Intern Med*. Feb 2002; 136(3): 243-246.
62. Association of Surgical Technologists. Core curriculum for surgical technology. 2011. http://www.ast.org/uploadedFiles/Main_Site/Content/Educators/Core%20Curriculum%20v2.pdf. Accessed June 30, 2015.
63. Association of Surgical Technologists. AST continuing education policies for the CST® and CSFA®. 2005. http://www.ast.org/webdocuments/CEpolicies/. Accessed June 30, 2015.
64. Pappas C. The adult learning theory-andragogy-of Malcolm Knowles. May 2013. https://www.elearningindustry.com/the-adult-learning-theory-andragogy-of -malcolm-knowles. Accessed June 30, 2015.