GET SMART

DIGITAL DEVICES IN DERMATOLOGY

BY **EMILY MARGOSIAN,** CONTENT SPECIALIST

Almost precisely 10 years ago, the first iPhone hit the consumer market in late June 2007. In the decade since, 2.3 billion people — or 32 percent of the current global population — have become smartphone users. Unsurprisingly, digital devices are no stranger to the dermatology office either. According to recent studies, approximately three-quarters of all health care providers use their smartphones as part of their practice, while a little more than half use tablets in their duties caring for patients. The shift toward smart, handheld tech isn't just limited to providers, however. Patients now use their mobile devices to make and confirm appointments, access medical records, and view their patient accounts.

While mobile devices in health care have streamlined administrative tasks and elements of patient care in some areas, they've introduced new challenges in others, particularly growing concerns around cybersecurity. *Dermatology World* consults with dermatologists and health care tech experts on how smart devices are carving out new roles in the areas of:

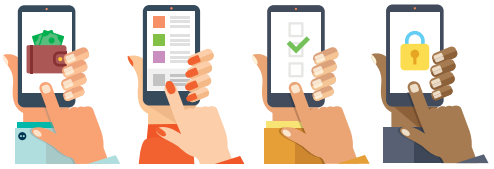
Payment processing

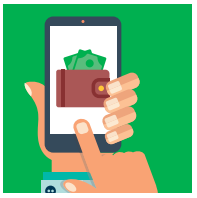
Patient education

Quality efforts and clinical workflow

Data security >>

GET SMART

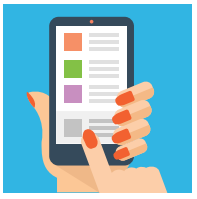




Streamline payment procedures

The medical practice front desk may be due for an update not unlike that of the airport check-in counter, suggests Medical Group Management Association consultant Derek Kosiorek in a recent *Physician's Practice* article. Just as airlines have moved to increasingly implement self-serve check-in kiosks for flights, according to Kosiorek the introduction of smart devices into medicine has enabled "practices to do real-time adjudication with the insurance company to determine what the copay is going to be before the patient goes into the exam room, or check insurance availability."

Tablets in particular can cut down time at patient check-in and check-out, streamlining a range of previously paper-based administrative tasks. Digital signature pads and tablets with built-in credit card swipes can be used to handle co-pays, and some manufacturers, such as PhreesiaPad, can also enable patients to enter and update personal or insurance information as part of the process. As EHR technology continues to evolve, depending on a practice's EHR system of choice, this information can potentially be automatically imported directly from the device into a patient's record.



Patient education

Beyond payment possibilities, digital tablets and smart screens can also be tools for disseminating key clinical information to patients in the exam room while an appointment is taking place. Laura DeStefano, DO, has implemented a full suite of digital educational content into her Port Charlotte, Florida, practice over the past year, leveraging it across digital waiting room screens, patient tablets in exam rooms, and interactive wallboards. "I have a background in teaching, so I spend a lot of time on education with patients," she explains. "Previously I was spending a lot of time drawing diagrams to explain what was happening at the cellular level. Now more often than not I'm using the wallboard to illustrate things like skin cancer or surgical treatments. Even the patients who have had numerous carcinomas removed in the past really have appreciated having a better understanding of what is being done and why."

Dr. DeStefano sources her technology and derm-related content from Outcome Health, which partnered with the AAD in November 2016 to co-produce dermatologic health content for patient use before and during consultations. The collaboration offers Outcome's full platform of digital technology to AAD members at no cost. (More information is available at **www.aad.org/practicecenter/managing-a-practice/affinity-partner-programs/outcome-health**.)

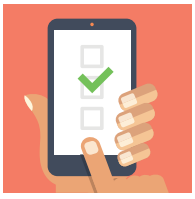
"Patients appreciate the trusted and credible information they receive from their dermatologists during in office-counseling, and research has shown the benefits of patient education, including greater treatment and compliance and overall patient satisfaction," said Rebecca Tung, MD, former chair of the AAD's Public Education Committee in a 2016 statement, a sentiment that's echoed by Dr. DeStefano. "The fact that Outcome Health has partnered with the AAD gives me confidence in the content that my patients are viewing when they're waiting in our reception area. We used to just have a short video loop that played on repeat; it's been a big improvement."

Michael Gutierrez, MD, a dermatologist in Orlando, Florida, says the implementation of Outcome's waiting room screens has been helpful in cutting down time spent answering questions in the exam room that could have been addressed earlier. "We have 25 office locations, and we've customized our screens to run photos of all our doctors and nurse practitioners, along with services that we offer," he explains. "It helps get the doctors' credentials out; it lets you meet the staff; it gives out information about Botox or fillers or other services that you're offering, so you don't have to spend time during the actual exam going over that."

Dr. Gutierrez's utilization of digital devices is limited primarily to his practice's reception area, however. "As far as sitting with a tablet with a patient going over something, I don't really see the upside of that," he says. "It seems to me it would be

more time-consuming than just verbally explaining to a patient what's going on."

For Dr. DeStefano, however, using the devices as tools to explain potentially difficult clinical concepts has delivered a noticeable patient satisfaction boost. "Younger patients tend to be active learners and really respond to the wallboard. I'll allow them to use the touchscreen, and I'll talk them through it as they activate the animation. The basic skin model is great for explaining anything from folliculitis to tinea," she explains. "I have found that patients are paying more attention, and using the devices as a springboard to ask questions that they may not have thought to ask previously about their disease, or to address a cosmetic concern they were not aware that could be corrected."



Quality efforts and clinical workflow

More screen time may make patients happy, but what about providers? While smart devices can be used for a variety of clinical purposes, for dermatologists it's a smartphone or tablet's dual function as both camera and computer that may come most in handy, especially when transferring photos into their EHR. "Dermatologists have the unique requirement amongst all medical specialties to capture and store standard photographic pictures of their patients," says Morris Stemp, CPA, MBA, CPHIMS, chief financial officer at StratX IT Solutions. "As essentially mini-computers, smartphones can run apps which facilitate the transfer of images from the smartphone onto a storage device, generally via Wi-Fi." Stemp recommends that any practice using Wi-Fi to wirelessly transmit photos should have their Wi-Fi security set to "a minimum of WPA2 to ensure compliance with HIPAA encryption and security requirements."

Beyond just snapping clinical photos, smart devices can enable dermatologists to share pertinent patient information with other authorized individuals, and allow for easier collaboration with a patient's other providers. For example, "a dermatologist may store an image in the cloud and enable another physician to view the image and provide a second opinion," says Stemp, "Or, using Google Drive for example, two doctors working from separate locations can simultaneously edit the same document."

Thanks to advances in cloud storage, much of this information can be accessed via a practice's smart device, providing that the storage vendor being utilized is HIPAA-compliant. Likewise, a practice can benefit from the scalability and mobility offered by cloud-housed storage. According to Stemp, the options are myriad. "Dropbox for Business, Box for Enterprise, Google Apps for Work, CentreStack software, and Microsoft OneDrive all advertise that they will sign a business associate agreement (BAA), and encrypt data, but only for their higher level plans."

Additionally, smart devices can help a practice to go paperless by utilizing digital signature technology to collect electronic consent for procedures and store patient signatures on practice policies. For doctors who have switched over from paper records to EHR, paper consent forms require manual scanning into a patient's electronic record. "The process of printing a consent form, filling in the name of the procedure, having the patient manually sign it, scanning the signed form, and then either filing or shredding the signed document is very time-consuming," says Stemp. "Documenting informed consent electronically can save time and effort."

Utilizing tablets to collect digital signatures can also help keep patient forms organized and definitively timestamped. "A lot of times doctors will give patients a whole slew of forms, but not all of them may be dated. The digital signature gives you your real, live authentication that a patient signed it on a specific date," says Stemp. Likewise, digital signature pads can be installed with features to better ensure patients are actually reading the forms they're signing. "With some of the newer technology, you can sort of force the user to actually read the document. Some will have time delays where it'll present the form to the user, and they won't be able to sign right away, but will have to wait a couple of minutes to look through the form," says Stemp, who recommends that practices have two general options when looking into collecting e-signatures from patients.

One involves purchasing a low-cost signature pad with a stylus and downloading the software required to create signature fields. Alternately, practices can invest in tablet-style devices directly from vendors offering signature pad solutions (such as Topaz, Wacom, ePadLink, Signotec, and Zignature Pad).

Steps to security

Hacking in health care is on the rise. Increasingly frequent media reports chronicle major hospitals and health insurers that have fallen victim to ransomware demands. According to a recent *Hill* report on the phenomena, cybercriminals "can tap into one weak point at a hospital — like an unsecured wireless printer — and access the entire system. Hackers can take over a hospital's electronic records or lock them out of their website and only return control after a ransom is paid, often in Bitcoin." Data also suggests that digital security should also be of increasing concern to providers. More than 113 million personal health records were compromised in 2015, according to the Department of Health and Human services (DHS). As such, arguably any dermatology office with an internet connection — but doubly so one that has made smart tech an important part of its workflow — should follow some key guidelines to diminish cybersecurity risks. A good mobile security arsenal should include:

- Regularly updated antivirus
- Long, strong passwords
- Multifactor user authentication
- Remote lock and wipe capabilities
- HIPAA-compliant storage
- Keeping business and personal use separate

Up-to-date software

While it might sound like a no-brainer, one of the first steps toward keeping devices secure is to keep them updated and installed with antivirus software. "Are the devices being kept current? Do they have the latest version of the security software or the device hardware? These are all things that help keep a device secure," advises Joe Mutlu, CIO at SCG Health, a health care consulting firm.

What's the password?

Beyond current software, the next question in any digital security lineup should be does the device use passwords? It should. "A good rule of thumb is seven to eight characters, using a capital letter, a lowercase letter, a number, and a special character," says Mutlu. "Obviously the more complex the better. Also helpful is if the devices are set to timeout after a set number of incorrect password attempts."

User authentication

Once your in-office devices are password protected, the next step is implementing multi-step authentication. "Does it use two-factor authentication, which is a password, and say a code? You'll see this done with banks where they'll verify by sending you a text message with a code to type in before you can access information," says Mutlu.

Screen timeouts are another form of user authentication, prompting users to re-enter the correct password after a set amount of time has elapsed between uses. "I usually recommend five minutes maximum," says Mutlu. "A lot of people don't like that because it's a pain to have to re-type in your password every time you put the tablet down for five minutes, but that tablet locking may be the thing that keeps it secure."

Remote lock and wipe

So what good are all those precautions if your device is lost or stolen? That's where lock and wipe capabilities come into play, allowing users to remotely freeze use or wipe personal information from a device remotely. "There are third party services that offer that. Apple has that capability with their devices; Microsoft offers that with some of their cloud services," says Mutlu. Installing remote tracking apps or software can also be critical in potentially recovering a lost or stolen device.

HIPAA-compliant storage

While your device may now be secure, what about the cloud storage you're using to upload data from your in-office smartphone or tablet? According

Bite-sized best practices for mobile device security

1. **Implement user authentication controls:** Providers should use any and all device locking mechanisms to secure devices used for work purposes. Locking devices with a passcode or biometrics can be a critical first line of defense in keeping data safe from unauthorized users.

2. **Enact remote and automatic lock and wipe capabilities:** These capabilities can be vital if a smart device containing patient information is lost or stolen, or after an excessive number of incorrect login attempts.

3. **Install security programs:** As hackers are now targeting mobile devices with the same intensity once directed at traditional desktops, it's increasingly important for physicians to install internet security software onto their mobile devices to prevent harmful apps or malware from compromising protected data.

4. **Employ encryption:** Overall, any data that is stored or transmitted via digital device should be encrypted. This extends to information exchanged via apps, email, and attachments.

5. **Develop an application policy:** For practices utilizing smart devices operated by several different users, it is vital for providers to understand the risks associated with harmful apps. Staff should be encouraged to seek approval for the installation of new apps on devices used for work.

6. **Encourage regular updates:** Updating operating systems regularly is a key component of any digital security strategy. Hackers target vulnerabilities in operating systems, and installing regular updates helps close any security gaps and keep data safe.

to Stemp, "I think the first question to ask is what makes a cloud storage system HIPAA-compliant?" As a rule of thumb, cloud storage vendors should meet three key criteria to meet HIPAA guidelines:

1. All vendors that work with providers and have access to protected health information (PHI) must sign a business associate agreement (BAA). Thus, any company that provides cloud storage must be willing to sign a BAA with the provider.
2. Data must be encrypted at rest and in transit. The cloud storage provider must offer this level of security.
3. The vendor must offer administrative controls to manage user access and permissions.

"When used wisely, cloud storage can be a cost-effective, flexible, and secure solution for storing data," says Stemp, "But providers should be careful to not consider cloud storage as a way to offload their practice's obligations to secure PHI."

Work devices for work-use only

Despite the best preemptive security safeguards, as always, the human component is often the greatest threat. "Devices that are encrypted and strictly used for business are about as secure as they can be. The problem is when devices are accessed by a physician's kid or used for personal use as well, and that's where you bring in all these other vectors of potentially being compromised," says Mutlu. "The more places the tablet goes, and the more people that use it, the more avenues for infection."

Mutlu advises that smart devices in a medical practice should be connected only to services and software being utilized in the practice setting, and that even so, safe browsing habits are key. "Many of the threats these days come in emails, or compromised webpages. You might be going to a perfectly good webpage, like a newsmedia or social media site, but the advertisement on that page may be compromised. Ultimately, smart devices are as secure as the person using them." ***dw***