PUBLICATION

Will the Continued Growth of Telehealth Shrink Our Information's Privacy? [Ober|Kaler]

January 01, 2015

The growth of telehealth and telemedicine services is inevitable. "At-your-fingertips" services are the status quo these days. From shopping and socializing to education and health care, flexibility and the virtual nature of services are almost standards expected from all types of service providers, and they provide a competitive edge touted over competitors. Health care service providers are no exception. Finding ways to improve patients' experience and satisfaction can not only expand a provider's patient base but also facilitate the earning of additional payment incentives. Offering telehealth and telemedicine capabilities often is such a way to achieve these goals.

While the terms "telehealth" and "telemedicine" often are used interchangeably, in the industry they are known to have distinct meanings. Telehealth generally refers to the broader scope of remote health care services beyond clinical services, such as education, access to medical records though patient portals, or administrative services. Telemedicine primarily refers to clinical services only. Keep in mind that these are general definitions and that Medicare, along with each state Medicaid program, commercial insurance payers, and state statutory or regulatory codes, may have its own definitions for these terms. In terms of telehealth, this article speaks to how the issues raised relate not only to clinical health information specifically but to all variations of an individual's health information.

With patients and providers increasingly interested in telehealth, we likely will see a growth in telehealth vendors and software providers. Telehealth systems may distinguish themselves from competitors in a number of ways, including the interface with telehealth providers (e.g., audio-only, video capability?) or with regard to when and how patients can access the system (At home? At work? Via personal computer/ laptop? Tablet? Smartphone? Or perhaps, the Apple watch?). Innovations in this area could help increase access to preventative care, decrease health care costs, and improve overall patient satisfaction. On the other side of the coin, however, are additional risks, such as a breach or improper use of a patient's information. Because the benefits of telehealth can be significant, providers and patients likely will be ready to accept the associated risks, for which they also must be prepared.

More Interchange of Electronic PHI = More Potential for a Breach of PHI

At base, the privacy concerns or potential risks related to the use of telehealth are the same as those associated with the use of any Protected Health Information (PHI), as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. Simply stated, the concern is that a patient's sensitive information will be used, disclosed, or accessed by an unauthorized person. Worse yet, such use, disclosure, or access will harm the patient in some way. Providers, such as physicians and physicians' groups, also face the risk of monetary penalties under HIPAA from a breach of PHI. Despite these potential risks, both physicians and patients continue to be interested in electronic communication and in a mobile and convenient way to communicate. While telehealth does not bring to the table any *new* HIPAA privacy issues or concerns, it does increase the opportunity for privacy issues to arise. Gone are the days when a patient's paper medical record was kept under lock and key in one physician's office. This article provides examples of the five key

elements (i.e., the Who? What? Why? Where? and When?) so that physicians and patients can continue to facilitate the use of telehealth, but also take steps to mitigate the privacy risks.

Who?

First and foremost, in the context of telehealth, the "who" is the patient, as it is the privacy of the patient's information that is at stake. From the outset, patients should be informed of the parameters of their use of telehealth systems and should be made aware of the inherent risks. Commonly, these risks relate to the confidentiality of usernames and passwords that enable access to the system. With such credentials, patients may log on to a physician's telehealth system and typically, see their medical record; future and past appointments, including, perhaps, the reasons for such appointments; and prior communications, such as emails with their physicians. Where a system does not include a video capability, physicians responding to patient inquiries on the other end can verify the patient's identity only by virtue of a successful login to the system. All the while, it is possible that someone, other than the patient, has obtained the credentials and accessed the system, as well as the patient's PHI, available through the system.

In this scenario, the physician often may not know about the improper access unless the patient is aware of it and informs the physician. Because physicians can do little to guard against this scenario (encryption is no help when the correct credentials are used), physicians should provide full disclosure to patients and require their clear acceptance of this risk. Disclosures and risk-acceptance acknowledgements can be routine aspects of initial telehealth sign-up forms.

What if the "who" is a minor patient? While the same risks are present, there is the added obstacle of ensuring minors' legal rights to, and the privacy of, their information is not compromised. HIPAA and certain state laws give minors the same autonomy and rights to their health care information related to certain services ("adult services") as given to adults. In effect, minors' parents do not have any rights to the information and no longer are the minors' "personal representatives" under HIPAA, unless the minors authorize their access to the information. Therefore, although the parent signed up for telehealth with the child's pediatrician for purposes of conveniently accessing the child's records or receiving a consult, the parent may be prohibited from viewing such information if it relates to an adult service. While frustrating for the parents, the burden and risk of a privacy breach rests with the physician. Should physicians choose to allow parents to access their child's information via a patient portal or telehealth system, the parents should have their own log-on credentials and be able to view only the information designated "non-adult services." Instituting such a safeguard and practice assumes, of course, that aphysician's system has such capabilities. Accordingly, in these situations, the first step likely is for the physicians to assess their system's ability to address the specific considerations raised by a minor's use. Some providers may determine it is not possible and/or not worth the risk and make the decision to not offer these types of telehealth services to a minor or a minor's parent.

What?

Within telehealth, the "what" can be many things, but a prominent aspect is the technology or the system used to facilitate the remote service. The increased use of portable and valuable mobile devices by both parties to the communication (patient and physician) naturally increases the risk of theft of the device and information. In addition, as patients continue to rely on this method of communication with their physicians as a standard, the communications will continue to reach beyond the primary care or nonemergency consult and will involve the full scope of information. Such exchanges will include reviews of films, test results, and scans—all on a mobile device (assuming, with regard to images, that the device has adequate capabilities to produce diagnostic quality images). Physicians should have strict policies and procedures in place for mobile device use and the security features that must be included, such as encryption. This is somewhat easier when the employing

facility or group provides and supports the devices, but when "bring your own device" (BYOD) is an acceptable practice, much of the control over such safeguards is lost. While BYOD may be a cost savings, physicians should consider whether it is worth the additional risk that comes with foregoing control over the security and use of the device.

Added to the "what" is the patient's mobile device. An appeal of telehealth is the flexibility for patients to communicate at their convenience, and mobile device use supports this. Unlike professional groups and institutions, a patient likely will not have a data management team supporting the patient's use of the device to ensure its security. If possible, within their telehealth system, physicians should consider limiting patients' ability to download information to their devices. While physicians cannot require patients to adhere to any mobile device policy, including any encryption requirements, they should make an effort to warn patients of the risks inherent in storing information on their mobile device. Again, it may be prudent to obtain patients' clear (and written) acknowledgement of such risks.

Why?

One "why" within telehealth is the reason for the remote visit or consult. Telehealth may have started with teleradiology, but its scope has expanded significantly, including general telehealth visits and consults with primary care physicians, tele-ICU, telestroke, teledermatology, telewound care, and telepsychology (telepsych). While telehealth proponents see this expansion as furthering the benefits of telehealth, from a privacy perspective, it also increases the risks. And these privacy-breach risks become more concerning when the nature of the information becomes more sensitive-for example, information collected via a telepsych consult. For this reason, some physicians may want to limit their use of telehealth to less-sensitive information exchanges, unless additional security protections are in place.

Video capabilities are another component of telehealth where additional scrutiny may be warranted. While these capabilities may be viewed as a key "value-added" feature to a telehealth system, they may pose more potential harm to the patient if breached, and therefore, may warrant additional safeguards from both a privacy and security standpoint.

Where/When?

The "where" and the "when" can be addressed simultaneously when they relate to the actual access and use of the telehealth system. Both the patient's and the physician's location and timing of access require some thought from a privacy perspective. While the most common place for patients to access telehealth services may be from home, employers increasingly are offering telehealth access to employees at work as a way to increase productivity and employee satisfaction. From the patient's perspective, this may raise some concerns. Does the patient have a private place to talk with the physician? Is the information stored on the employer's servers? How does the impact of a breach change within the context of the employment setting? Patients may feel their privacy even more compromised in a breach if their employer learns of a diagnosed illness, as opposed to a stranger trolling for financial data. As another example, suppose that during a telehealth consult, which was audio or video recorded, an individual discusses negative feelings towards her employer's sick leave policies. Any disclosure of that recording within the workplace would be, at best, awkward.

Employers offering telehealth in the workplace should notify employees of the limits to the privacy of the information they choose to share via telehealth in the workplace. As the situation dictates, the employer should remind employees that the same employer policies and procedures related to communications apply to telehealth communication. Such policies often convey that employees using employer-owned equipment should have little expectation of privacy of the information transmitted through that equipment. While such

policies initially targeted email, Internet, and social media use, they would now apply to an employee's sensitive health information.

"Where" and "when" also apply to the physician's use of the telehealth system. While we may think of a physician on a video screen in her white coat talking to the patient from her office, that may not be the case. Mobile technology enables the physician to communicate while in a facility common area, making rounds, outside, or perhaps, even at home. As noted above, this increase in convenience comes with additional opportunity for unintended disclosures of a patient's sensitive information. While these risks may seem manageable, physicians should still weigh the benefits against the risks to determine if they are worth taking. As an aside, even if physicians feel they have free rein to use the system wherever the platform allows, they may decide that a location other than a physician's office or hospital does not convey the desired professional tone to patients.

Conclusion

Undoubtedly, telehealth use will continue to grow in the physician/patient relationship. As telehealth vendors develop new capabilities for even more flexibility and access opportunities, it is important to keep in mind the additional level of risks associated with these developments as far as privacy control and monitoring. While legal counsel and compliance officers are not always involved in most vendor or service-arrangement negotiations, incorporating them into these types of discussions at the outset to spot potential issues with the Who? What? Why? Where/When? may be one of the best safeguards against acceptance of unnecessary risk.