ANNALS OF CLINICAL PSYCHIATRY 2017;29(4):217-218

GUEST EDITORIAL

Perils and limitations of modern-era medical communications

Richard Balon, MD
Departments of Psychiatry and Behavioral Neurosciences and Anesthesiology
Wayne State University School of Medicine
Detroit, Michigan, USA

CORRESPONDENCE
Richard Balon, MD
Department of Psychiatry and Behavioral Neurosciences and Anesthesiology
Wayne State University
Tolan Park Building, 3rd floor
3901 Chrysler Service Drive
Detroit, MI 48201 USA

E-MAIL
rbalon@wayne.edu

Over the last quarter century, modern technology has brought us new methods of communication—e-mail, texting, and social media, including Facebook, Instagram, and Twitter. The medical community has gradually adopted these methods. They are quick, convenient, and used by almost everybody, which creates an added pressure to use them. Many physicians use these tools for communicating without thinking much about the perils and limitations of these formats in transmitting medical information among medical professionals or between doctor and patient. The quickness and ease of electronic communication is seductive: It allows us to get or send information *right now*, without any delay, no matter where we or the other party are located. Unfortunately, communication happens frequently without considering what is allowed through these means, the risks of breaching confidentiality, and how to avoid (or, more correctly, to mitigate) risks. Confidentiality also could be violated accidentally, such as using a wrong e-mail address or telephone number. Let's also not forget that any phone, social media account, or e-mail address could be hacked.

These new ways of communication also may lead to blurring or violating boundaries. A physician may look for information about a patient on the Internet (not a good practice), and a patient may do the same, or social media contacts may lead to "friending" of patients. The latter situation could be especially troublesome: Is the patient a "patient" or a "friend?" Does answering a clinical question via Facebook constitute treatment?[1] Patients also may feel as if this communication is intimate and confidential,[1] which it is not.

In addition to convenience and quickness, there are other positive aspects of communication with patients via e-mail, texting, or, to a lesser degree, social media. Patients like it, and it saves time, avoids "phone tag," and may strengthen the therapeutic alliance.[1]

Nevertheless, we are clearly walking in a minefield of possible mishaps, complications, boundary violations, and ultimately violations of the Health Insurance Portability and Accountability Act (HIPAA).

The question is how to prevent complications, and what to do about the risks. There are 2 areas—communication with patients, and communication with colleagues and other medical professionals—that may call for different approaches, but ultimately we have just 1 relatively acceptable solution: the de-identification of the data communicated. With regard to communication with patients, we can decline to give them our contact information. It may be relatively easy to refuse to divulge one's mobile phone number or Facebook contact (and I would strongly advocate for it), but not giving one's e-mail address is a bit unrealistic because it can easily be found through various means. As far as communication with colleagues or other medical professionals is considered, we probably would not refuse to give out a phone number and e-mail address, but we probably should not share a Facebook contact with everybody.

Nevertheless, these solutions are not satisfactory because (a) as noted, any account can be hacked, and (b) our communications should be HIPAA-compliant. However, as Drolet[2] pointed out, "Because HIPAA is technology neutral, there are no meaningful standards." He also noted that HIPAA requires that communication addresses security by identifying "reasonably-anticipated risks" of breach and creating mitigation strategies. These could include strong passwords, message and operating system encryption, and remote deactivation capability for lost or stolen devices. Drolet[2] also stated that HIPAA compliance could be maintained by de-identifying the information transferred and listed 18 types of patient identifiers that have to be removed, according to the Safe Harbor Method.[3] These are account numbers; all dates (except for the year) related to an individual (eg, birth date, admission date); biometric identifiers (eg, fingerprints); license or birth certificate numbers; serial numbers or medical number identifiers; electronic mail addresses; fax numbers; full face photographs or specifically identifiable images; geographical location or subdivisions smaller than a state; health plan beneficiary numbers; Internet protocol addresses; medical record numbers; names or any derivatives, including initials; phone numbers; social security numbers; vehicle identifiers (eg, serial numbers, license plate numbers); web universal resource locators (URLs); and any other unique identifying number, characteristic, or code.

This de-identification seems cumbersome, but it is possible in communication between medical entities, especially when combined with addressing other aspects of security (eg, strong passwords). But what about communication with patients? Some communications, such as appointment reminders, refills requests, short answers to short questions (eg, side effects), and short updates by the patient may be appropriate.[1] It may be better to limit or avoid anything beyond that. The rules of such communications should be established up front, and the patient should consent to this method of communication. The risks should be discussed. It should be clear who reads the communication.[1] Last but not least, all communications should be filed (eg, I copy all my e-mails with patients into their electronic medical record).

Modern-era medical communications are easy, convenient, quick, and here to stay. We have to be vigilant about the way we communicate among ourselves and with our patients, because the perils and limitations of these communications are significant. We also should realize that there is no obligation to respond to an unsolicited e-mail or friend request via Facebook or other social media. ■

REFERENCES

1. Mossman M. Medicolegal hazards in the information age: malpractice and more. Presented at: Psychiatry Update 2017: Solving clinical challenges, improving clinical care; March 30, 2017; Chicago, IL.
2. Drolet BC. Text messaging and protected health information. What is permitted? JAMA. 2017; 317:2369-2370.
3. U.S. Department of Health and Human Services. Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. https:/www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification. Published November 26, 2012. Accessed July 1, 2017.