Status Update: Social Media Exchanges are Sometimes Part of the Health Record

By Dana C. McWay, JD, RHIA, and K. Jody Smith, PhD, RHIA, FAHIMA

Now that physicians are offering medical advice over e-mail and social media, HIM must reexamine processes for a complete and accurate health record

Imagine you are a physician who has been corresponding with an established patient via e-mail. The patient has provided you with symptoms that appear to meet the definition of a skin rash. The patient has even provided, via e-mail attachment, a photo of the rash, which confirms your suspicion that a skin rash diagnosis is appropriate. You prescribe a topical agent that can only be obtained through a pharmacy and advise the patient to apply it on a scheduled basis. Should this e-mail correspondence become part of the patient's health record?

Or imagine you are a physician who authors a blog on behalf of your healthcare institution. Total strangers create posts on the blog asking for advice to address their health concerns. You address these concerns by providing medical advice. These strangers continue to create posts, informing you of the results they achieved based on your medical advice. Where appropriate, you provide further advice to address remaining medical issues and problems. Should these blog posts become part of a patient's health record?

While the better practice may be to refrain from using these technologies to provide medical advice to patients, situations like these have become far more common in today's healthcare environment than ever before. The proliferation of social media technology, including—but not limited to—blogs, wikis, instant messaging, social network platforms, online forums, and video/image sharing sites, has changed the way the world communicates. More traditional forms of technology such as e-mail and text messaging have also changed our communication habits.

The speed with which people can communicate using social media technology has helped to popularize it. And that popularity has caused many healthcare practitioners to adopt these technologies not only for their personal use, but also for their professional use. When electronic protected health information (ePHI) is created, received, or exchanged as part of patient interactions using social media technology, it is important to create a patient care record to adequately document the interactions.[1]

There are several reasons why patient-provider contact using social media technology may necessitate creating a patient record or adding to an existing patient record. There are issues related to information governance, proper record practice for electronic communications, and legal concerns that require health information management (HIM) professionals to be knowledgeable of how and when social media communications become part of a patient's health record.

Information Governance Applies to Social Media

Information governance refers to the coordinated, interdisciplinary approach to satisfying and managing information-related practices, requirements, risks, and opportunities while optimizing information value.[2] Information governance addresses the accountability framework and decision rights necessary to achieve enterprise information management and focuses on multiple disciplines, including records and information management.[3] Information governance establishes the structure for determining what information should be retained, the integrity of that information, the manner and time periods in which it is retained and stored, and the appropriate procedures to be followed when disposing of physical and electronic information.

In the context of patient-provider contact using electronic technology like social media, information governance principles are being used to address this new HIM territory. With regard to the information exchanged in the above examples, the first step to determining if it should be included in the health record would be to apply an information governance review. This review

would specifically focus on the type of information exchanged and whether that information constitutes medical advice and/or clinical data.

In the two earlier patient-provider communication examples, the shared content consists of medical advice, which is defined as the provision of a professional's opinion about what action an individual should or should not take with regard to their health.[4] This advice is in contrast to medical information of a general nature, which is not specific to a particular patient's situation and is accessible to many persons. Medical advice that is personalized and relates to a specific patient's health and course of treatment and care is considered clinical data.[5] As such, clinical data warrants review under information governance principles as to whether it should be included in the health record.

In the previous examples, bi-directional information flows between the patient and the physician that contains medical advice and that has been relied upon by the patients to advance their treatment. These examples are not simple, innocuous interactions without substantive content related to patient care. Accordingly, an information governance policy is needed to address both examples to determine what information exchanged should be retained, how to maintain its integrity, how the information should be retained and stored, and how it should be disposed of in the ordinary course of business. Such decisions include deciding how this information will be added to a patient's health record, retained, and stored.

Proper Record Practices for E-mail and Text Messages

Research conducted by wireless communication association CTIA revealed 2.19 trillion text messages were sent in 2012.[6] Also, a 2012 National Health Survey by Penn, Schoen, and Berland indicated that 75 percent of those surveyed had sent their physician an e-mail or text message during 2012, and 54 percent indicated they wanted e-mails or text messages with health reminders from their healthcare provider.[7] Physicians are also exchanging text messages with colleagues to support patient care in the form of patient referrals, medical notifications, request for consultations, order clarifications, and discharge instructions.[8] These findings demonstrate a shift in the way people communicate, moving from face-to-face or telephone contact to electronic methods.

Stage 2 of the Centers for Medicare and Medicaid Services' "meaningful use" EHR Incentive Program requires healthcare providers to implement a patient portal that allows patients to access their health records and take an active role in their healthcare by making informed decisions about their care.[9] The patient portal allows patients access to their personal health information and health records through a secure online website. Features available through the portal may include retrieving diagnostic test results, requesting prescription refills, scheduling non-urgent appointments, and exchanging secure e-mails with the healthcare team.[10] Because the patient portal is secure, communication exchanges between the patient and the healthcare team can become a permanent part of the electronic health record. When e-communication is sent outside secure means, privacy and security experts advise healthcare providers to use the unsecure e-mail only as a means to refer the patient to the patient portal in order to obtain the desired content.[11]

HIM professionals should note that the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule does not distinguish between face-to-face communication and electronic communication. The Privacy Rule allows electronic communication between the patient and covered healthcare providers as long as reasonable safeguards are used during the exchange, such as verifying the recipient's e-mail address. Electronic communication initiated by the patient and sent to the healthcare provider is acceptable as long as the patient understands the risk of using unencrypted e-mail. It would be prudent for the healthcare provider to make the patient aware of these risks prior to communicating electronically.[12]

Another frequently used approach to exchanging electronic protected health information (ePHI) involves the use of text messaging. Any such exchange should follow HIPAA safeguard protocols for the exchange of electronic transmissions. Such protocols require the use of appropriate security safeguards, such as encryption of data and use of secure private servers.[13] The difficulty lies with the realization that any text message must go through a cellular provider, who may or may not sign a business associate agreement required under HIPAA and may store data in locations outside the control of the healthcare provider. For these reasons, great care should be exercised when deciding whether to use text messaging to exchange ePHI.

Social Media Legal Concerns

Legal implications exist when communication technologies are used by a provider and patient as part of patient interactions. Some implications include whether a provider-patient relationship has been created, the application of HIPAA, the role of electronic discovery (e-discovery), and the business record exception.

In the two examples provided at the beginning of this article, each involves an instance of a provider-patient relationship. Upon first reading, it appears the relationship in the second example involving the blogging physician is not as clear because the description involves total strangers posting comments on a blog. Nonetheless, the physician has arguably established the provider-patient relationship by providing the posters with a response specific to the "patient's" situation.[14] By creating this provider-patient relationship, the provider establishes a level of professional responsibility for the patient. The failure to exercise that professional responsibility may lead to liability for claims of professional misconduct or malpractice if the advice provided results in a negative outcome for the patient. Additional claims may be made for the unauthorized practice of healthcare in a state that the provider is not licensed, and medical abandonment if the physician does not properly terminate the relationship with the patient following the social media interactions in these examples.[15]

Both examples raise questions of compliance with HIPAA. ePHI has been exchanged but there is no indication the patient assented to treatment through a patient authorization, thereby creating a potential privacy compliance issue. The types of media used in these examples are not HIPAA-compliant in a security sense, such as using encryption technology to meet security standards, or using HIPAA-compliant secure networks. The media used are the equivalent of a postcard that is available for anyone to read.

If genetic information is present in these exchanges, this genetic information may be used by a reader for a discriminatory purpose in violation of the Genetic Information Nondiscrimination Act (GINA).[16] It is likely that the physician in each example is not aware that the actions described violate HIPAA, GINA, or both, but the informality and lack of a professional atmosphere present with e-mail and many forms of social media technology makes it easy to lapse into conversations that are in reality protected by HIPAA and GINA.

Additional concerns are present because of the role of e-discovery. E-discovery refers to the process of seeking, obtaining, and preserving information stored electronically in any medium.[17] This form of discovery involves not only what is considered the traditional legal health record in electronic form, but additional data such as smartphone messaging and e-mail records. E-discovery also includes the raw electronic data that can be used for metadata analysis, including log-on and log-off times, what entries were made and when, and what changes were made and when. Virtually anything that is typed or e-mailed creates a permanent record that is subject to discovery in a lawsuit. The two social media exchange examples in this article clearly fall within the purview of e-discovery, enforcing the importance of adding these exchanges to the patient's health record.

Finally, the Federal Business Records Act's business record exception to the judicial hearsay rule will likely apply to permit the ePHI present in the two examples to be admitted into evidence if the foundation requirements of the rule are met. The business record exception allows the admission of a record into evidence if it is created and kept in the ordinary course of business at or near the time the event was recorded and by a person with knowledge of the acts, events, conditions, opinions, or diagnoses appearing in it.[18]

In both of this article's social media examples, the foundation requirements are met. The physicians' actions are conducted as part of the ordinary course of business—regular e-mail correspondence with a patient and authoring a blog on behalf of a healthcare institution. Both examples include the real-time recording of the physician-patient interactions and are completed by a person with the requisite knowledge—the physician. While the physicians in each example may not readily recognize that they have created a business record, the medical advice they provide makes the conversations qualify as business records and this advice should become part of a patient's health record.

To underscore the importance of including this medical advice in a patient's health record, consider the scenario addressed in the sidebar "Scenario: Medical Advice Gone Wrong" on page 29. The legal ramifications of excluding this medical advice may very well influence or result in the outcome outlined in this scenario. The better course of practice to avoid this legal ramification is to include the medical advice in a patient's health record.

Role of HIM Professional with Social Media Records

HIM professionals are the recognized experts in the collection, maintenance, and dissemination of health records. Knowledge of healthcare finance, legal aspects, coding, leadership, management, research, and data analysis provide a strong foundation for the HIM professional to assume a leadership position as healthcare transforms from a paper-based system to an electronic one. This transition is occurring rapidly, requiring the HIM professional to commit to lifelong learning and attain the knowledge, skills, and competencies needed to be a valued asset across the healthcare continuum.

HIM professionals understand the need for a complete and accurate health record that complies with the requirements of statutory provisions, accrediting agencies, state and federal administrative regulations, institutional standards, and professional guidelines. Because of their expertise in these areas, HIM professionals are the logical central points of contact for developing uniform policies and procedures to facilitate compliance with external and internal standards. Part of this effort must examine the use of e-mail and social media technology that provide medical advice to patients.

The presence of this clinical data in e-mail and social media technology should cause healthcare providers and HIM professionals alike to realize the need to document these interactions in a patient's health record. Just because the media used is different from a face-to-face patient visit does not mean that care is not being provided in these formats. Accordingly this care should be memorialized in the patient record.

With the HIM professional's assistance, healthcare providers can determine which pieces of clinical data obtained or generated as a result of e-mail and social media interactions have a place in a patient's health record and where within the record that clinical data should reside. This requires that each piece of clinical data should be reviewed and managed to ensure compliance with required records standards. Those pieces of data that do not constitute clinical data will likely not rise to the level of being placed in the patient's health record, and decisions can be made whether to retain that data by means other than the patient's health record or to dispose of it.

Regulate All Personalized Social Media Content

A fine line exists between providing specific medical advice and providing more generalized medical information in the relatively public forums of e-mail and social media. Social media and related technology are the very opposite of "private," and discussing sensitive subjects such as an individual's physical and mental ailments means personalizing content. This personalization of content and its exchange through electronic means brings into play the requirements of HIPAA, accrediting standards, administrative regulations, institutional standards, and professional guidelines. Each of these requirements addresses the content of the patient health record and should be considered when determining when to create or add to a patient's health record the physician-patient interactions involving e-mail and social media technology.

Informing this activity are principles of information governance, proper record practice for electronic communication, and legal concerns. The person holding the most expertise for this activity is an organization's HIM professionals, who can address the need for a complete and accurate patient health record that includes all clinical data relating to a patient.

Notes

1. Department of Health and Human Services. "Electronic Code of Federal Regulations." 45 C.F.R. §164.105(a)(2)(i)(D) (2014). http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr164_main_02.tpl.
2. Sedona Conference. "The Sedona Conference Commentary on Information Governance 2013." December 2013. https://thesedonaconference.org/download-pub/3319.
3. Warner, Diana. "IG 101: What is Information Governance?" *Journal of AHIMA* website. December 4, 2013. http://journal.ahima.org/2013/12/04/ig-101-what-is-information-governance/.
4. Definitions.net. "Definitions for Medicine." December 2013. http://www.definitions.net/definition/medical advice.
5. McWay, Dana. *Today's Health Information Management, An Integrated Approach*, 2nd edition. New York: Delmar, Cengage Learning, 2014, p. 124.
6. CTIA. "Your Wireless Life." 2013. http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts.
7. Penn, Schoen, and Berland Associates. "National Community Health Survey." *The Atlantic*. March 2013. http://atlanticlive.theatlantic.com/pr/CommunityHealth/PollResults.pdf.
8. Malkary, Gregg. "Secure Messaging Enhances Clinical Communications and Collaboration." Spyglass Consulting Group. October 2012. http://www.cortext.com/sites/cortext.com/files/resource-

files/Spyglass_Secure_Texting_Whitepaper.pdf.
9. Shapochka, Andriy. "Providers Turn to Portals to Meet Patient Demand, Meaningful Use." *Journal of AHIMA* website. August 23, 2012. http://journal.ahima.org/2012/08/23/providers-turn-to-portals-to-meet-patient-demand-meaningful-use/.
10. Office of the National Coordinator for Health IT. "What is a Patient Portal?" HealthIT.gov. http://www.healthit.gov/providers-professionals/faqs/what-patient-portal.
11. Shapochka, "Providers Turn to Portals to Meet Patient Demand, Meaningful Use."
12. Department of Health and Human Services. "Health Information Privacy FAQs: Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?" HHS.gov. http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570.html.
13. Centers for Medicare and Medicaid Services. "The Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs: Stage 2 Toolkit." CMS.gov. February 2013. http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_Toolkit_EHR_0313.pdf.
14. McWay, *Today's Health Information Management, An Integrated Approach*, pp. 67.
15. McWay, *Today's Health Information Management, An Integrated Approach*, pp. 65, 67.
16. Genetic Information Nondiscrimination Act. 42 U.S.C. §1320d-9 (2014).
17. Sedona Conference. "The Sedona Conference Glossary: E-Discovery & Digital Information Management, 3rd edition." September 2010. www.thesedonaconference.org.
18. Federal Business Records Act, 28 U.S.C.§1732(a) (2014) and FED.R.EVID. 803(6) (2014). http://www.gpo.gov/fdsys/.

Dana McWay (danahimlaw@aol.com) is a court administrator in the US federal court system, a director of the AHIMA Board of Directors, and serves as adjunct faculty in the master's of health informatics program at Saint Louis University. K. Jody Smith (smithjk@slu.edu) is a professor and chair of the health informatics and information management department at Saint Louis University.

Article citation:
McWay, Dana C; Smith, Jody. "Status Update: Social Media Exchanges are Sometimes Part of the Health Record" *Journal of AHIMA* 85, no.3 (March 2014): 28-32.