



© 2010 American Health Lawyers Association

April 30, 2010 Vol. VIII Issue 17

PHI Faux Pas: Social Media And The Unauthorized Disclosure Of PHI

By Barry Herrin and Trey Ingram, Smith Moore Leatherwood LLP

The social network of many present-day Americans is maintained, in part, through the collection and dissemination of information over a number of online social media platforms. Such practices, however, leave unwary healthcare providers and professionals at significant risk of inappropriately disclosing patients' protected health information (PHI). In fact, the widespread usage of user-friendly platforms that encourage people to share information with one another is making it increasingly difficult for providers to prevent the unauthorized disclosure of PHI. It is of paramount importance that providers understand the consequences of their—and their employees'—online interactions and take appropriate precautions to ensure that they and their staff do not violate the privacy rights of their patients.

This article addresses only a few of the many ways in which PHI can be disclosed inadvertently to the public through online social media, including "friending" patients, "tagging" patients, and "blogging" patients. Each section also offers practical steps providers should take to protect against such unauthorized disclosures.

Friending Patients

Few healthcare providers, if any, want to be known for having poor bedside manners; indeed, most providers emphasize customer service to non-clinical and clinical staff alike. However, providers must make clear to all members of their work forces that appropriate, in-person social pleasantries with patients and families do not extend into the online world of social media.

To “friend” (using the word as a verb) a person is to request a connection or affiliation through that person's online profile using a social media platform (e.g., Facebook, MySpace, etc.). If the request to connect is accepted, the site then identifies the requestor as a friend (using the word as a noun) or follower. When a healthcare provider creates a social media profile, either as a corporation or as an individual professional, the provider will be encouraged to “friend” patients through this platform, and patients may be encouraged to friend the provider, as well. Although registering with a social networking site and agreeing to be a patient’s “friend” may appear to be within the societal norm, before engaging in such conduct providers should carefully consider the Health Insurance Portability and Accountability Act (HIPAA) implications of online interactions with patients.

Although it depends somewhat on the platform and individual profile and privacy settings, a person’s online friends typically are able to identify one another as friends of the person. In some cases, the public at-large is able to determine the identities of a person’s online friends. In this regard, one potential pitfall for providers who have “friended” a patient is the possible assumption by other users of that social networking site (who may be unknown by and not connected to the patient) that the patient is in fact a patient of the provider. This assumption alone might create a violation of HIPAA, as the mere existence of a physician/patient relationship in some situations can be considered PHI. Providers should prevent this problem from arising by requiring potential online friends to agree to a written statement or indicate that they have read an online disclosure before an online “friendship” with the provider can be established.

Tagging Patients

A popular feature of some online social media platforms is the ability to publish photographs and “tag” (i.e., identify) people appearing in the photos. It is surprisingly easy to upload a photo through any of the various online social media platforms; doing so takes only a couple of clicks of the mouse, and entire online photo “albums” may be uploaded with just a few clicks.

The ease and popularity of uploading and viewing photos online has fostered an environment in which protection of individual privacy is hardly given a second thought, and it is rare that someone questions whether it is acceptable to post a photo for the online world to see. However, healthcare providers must guard against online posting of photos of patients, particularly where those photos depict patients inside a healthcare facility (e.g., a hospital room) or receiving treatment. This is a serious concern regardless of whether the patient is “tagged” in the photo.

Consider the following illustration: a hospital nurse, who has treated a patient for an extended period of time and developed a friendly relationship with the patient, has her picture taken with the patient. Thereafter, the patient passes away. Grieved by the loss, the nurse posts the picture online through one or more of her social media accounts, and she adds a caption to the photo—or perhaps updates her “status”—indicating that she is saddened by the passing of her “favorite patient” that day. Although the nurse’s action might be the online norm for a purely personal relationship, it is entirely inappropriate in the context of a professional relationship involving a patient and a provider. In addition, the caption or status update constitutes a violation of HIPAA due to the nurse’s unauthorized disclosure of the patient’s PHI (which may include the patient’s date of death, cause of death, the fact or nature of treatment, etc.).

Blogging Patients

There is a significant amount of detailed, intimate information that is now commonly self-reported (self-posted) online by bloggers, despite the private nature of such information. A scroll through modern blogs often reveals extraordinarily personal information about a person or that person’s associates that previously might be found only in a locked diary hidden in a secret desk compartment.

It is no longer uncommon to find patients blogging about the details of their medical conditions and treatments received. A naïve healthcare provider using online social media might assume that a blogger, by posting such information online, is somehow waiving his or her right to have the provider continue to safeguard the privacy of the blogger’s PHI. The provider might then imprudently post an online reply to the blogger discussing the procedure or the nature of the recovery or the blogger’s condition. Alternatively, the provider might post an unsolicited comment on the patient’s webpage discussing her PHI, thinking that the provider’s open discussion of the patient’s PHI is acceptable to, and has been implicitly authorized by, the blogging patient. Providers should not, under any circumstances, make such assumptions, because such online responses violate the patient’s privacy rights under HIPAA.

Healthcare providers have a continuing obligation to protect PHI following treatment of a patient, and this obligation is not destroyed by a patient’s self-disclosure of the PHI to an online audience. A provider who discloses PHI it obtained or created in treating the patient without the patient’s specific authorization to do so violates HIPAA, even if the patient has publicly discussed the same or similar information with numerous others. Although a patient’s self-disclosure of PHI might affect a claim for damages against the provider based on the provider’s privacy violation, it does not nullify the violation. Providers should be careful not to comment online about a patient, either intentionally or inadvertently, without the patient’s express written authorization to do so.

Protect PHI

Online social media have created a host of new legal issues to which the judiciary must interpret and apply law that predates the networked world. Within the last few years, and with growing frequency, we have seen social media addressed in criminal trials, judicial ethics scandals, and various employment contexts. One area that certainly appears ripe to be next on the docket is the disclosure of PHI through online social media. HIPAA violations are inevitable unless healthcare providers implement and enforce detailed social-networking policies and integrate those policies with their human resources disciplinary policies.

Barry S. Herrin, FACHE, Esq. is a partner with Smith Moore Leatherwood LLP. He regularly represents healthcare providers in all segments of the industry and advises on a wide variety of regulatory and operational issues, including hospital and healthcare operations and compliance, medical information privacy and confidentiality, informed consent, and advance directives and “right to die” issues. He is admitted to the bars of Florida, Georgia, and North Carolina, is a Fellow of the American College of Healthcare Executives, and is a Candidate for Fellowship in the American Health Information Management Association. Mr. Herrin received both his undergraduate and law degrees from Georgia State University in Atlanta, graduating each time with honors. He has served as a faculty member for numerous state and national meetings and symposia across the country and has authored or co-authored numerous articles on health law compliance for regional and national publications. He also edits Smith Moore Leatherwood’s e-newsletter on health information management and technology issues, [LegalHIMformation®](#). Mr. Herrin is an Eagle Scout and volunteers his time to the Boy Scouts of America and to the Civil Air Patrol, in which he serves as the National Legal Officer.

Robert S. (“Trey”) Ingram, III, Esq. is an associate attorney with Smith Moore Leatherwood LLP. His practice primarily focuses on litigation issues involving the management of electronically stored information, especially in the context of data security, privacy protection, and electronic discovery. Mr. Ingram has authored articles on electronic information contained in handheld devices and making electronic information reasonably accessible to party litigants. He is admitted to the bars of North Carolina and South Carolina.