June 3, 2014

HIPAA Back-to-Basics Bulletin Series
HIPAA Compliance in the Social Media Era

This is the fourth in a series of bulletins going "Back to Basics" on HIPAA compliance. With the recent changes to HIPAA resulting from the Omnibus Final Rule, this is a good time to reevaluate your organization's compliance with all aspects of HIPAA compliance.

In relatively few years, the lines between the physical and online lives of many people have blurred to a staggering degree. Millions - if not billions - of individuals, including many of your employees, physicians and patients, now spend a significant amount of time communicating, socializing, reading, learning, sharing, networking and playing through various forms of social media.

The uses and types of social media continue to evolve at a phenomenal pace. The health care industry is not immune. In fact, social media poses a unique set of issues for health care organizations to address, in addition to an already long list of general business considerations.

The Intersection of HIPAA and Social Media

In other industries, the consequences of an employee's inappropriate social media post may be limited to compromised proprietary information and/or bad publicity. Thanks to HIPAA and state medical privacy laws, the consequences for hospitals and health plans can be much more severe. The posting of protected health information (PHI) online without patient authorization will likely constitute a PHI "breach" that invokes HIPAA's breach notification requirements and subjects the hospital or health plan to an investigation and potential civil monetary penalties.

Under the Omnibus Final Rule, an unauthorized disclosure of PHI is now **presumed** to be a breach unless it can be demonstrated that there is a low probability the PHI has been compromised. This is a difficult standard to meet for any disclosure via social media due to the size of the potential audience and the difficulty in mitigating the effects of such disclosures. Even if a social media post is quickly removed by the user, it may have already been saved by countless viewers via the computer or mobile device's screen print function. These saved files can then be transmitted to others in a matter of seconds via text messaging or email.

Over the past three years, the U.S. Department of Health and Human Services has announced HIPAA breach settlements requiring covered entities to pay more than $1 million. While none of these settlements concerned a social media-related breach, it is only a matter of time until such a breach results in a settlement or civil monetary penalty.

Common Pitfalls

The posting of patient photographs, which can quickly be taken with a smartphone or tablet and uploaded to a social media site, is a common pitfall. While employees may be sensitive to posting textual PHI to social media, they may not realize that any photo that identifies an individual also constitutes PHI. Further, a photo does not necessarily need to include the patient's face for it to identify the patient (e.g., identification bracelets and birthmarks).

A second common pitfall is the "friending" of patients by health care providers, which indicates to third parties that the patient received care at the provider's facility. It is recommended that, when the only relationship between two individuals is that of patient and health care provider, the health care provider should not "friend" the patient on social media sites. However, if the individuals had a previous relationship (e.g., neighbors or friends), "friending" is acceptable, but the health care provider should be especially careful not to share any information regarding the patient's treatment.

Another issue frequently raised by employees of health care organizations concerns the supposed "mixed messages" that employees receive on the topic. On one hand, they are warned not to post PHI to social media. Meanwhile, they see the organization's marketing department post detailed patient stories with photographs to the organization's official social media pages. The difference, of course, is that the marketing department has obtained a HIPAA-compliant written authorization from the patient or his or her personal representative before posting any PHI to social media.

Recommendations

A written policy is a useful tool for addressing the various issues social media presents for your organization. To be of value, however, such a policy must be unique to your organization. Additionally, it must be carefully considered, drafted and periodically revisited so that it continues to make practical sense and remains compliant with applicable law.

With or without a policy, do not underestimate the benefit of social media education and training for your employees. Your employees may understand their obligations under HIPAA, but do they appreciate the HIPAA implications of posting patient photographs on their social media pages? Do they understand why the marketing department may post patient stories, while other employees may not? Through training, you can provide needed guidance to your employees and help protect your hospital against the growing threat of HIPAA liability related to social media use.

INCompliance offers customized HIPAA consulting services, including training programs and policy and procedure development that include social media components. Click here for additional information on our services.

This E-Alert was prepared by Chris Bennington. Chris can be reached 513.870.6572 or cbennington@incomplianceconsulting.com. Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com. This E-Alert may be accessed on the INCompliance website.