



NO-NONSENSE
RULES TO ENSURE
A HIPAA-COMPLIANT
SOCIAL MEDIA STRATEGY



A GUIDE FOR HOSPITALS

BY DAVID HARLOW JD MPH, THE HARLOW GROUP LLC
DAN HINMON, HIVE STRATEGIES

Some hospitals are allowing HIPAA anxiety to keep them from embracing social media platforms such as Facebook, Twitter, YouTube, LinkedIn, Foursquare and blogs.

There are now more than 900 U.S. hospitals engaging patients through social media; that means there are over 5,000 U.S. hospitals that have yet to take the plunge. Concern about exposure to liability holds back many hospitals, but there is solid information to keep you on firm ground, if you follow these nine no-nonsense rules.

Understand HIPAA *Page 3*

Consult with legal advisors *Page 4*

Limit liability *Page 5*

Train your staff *Page 6*

Do not practice medicine online *Page 7*

Take conversations offline *Page 8*

Prominently post your policies and procedures *Page 9*

Regularly monitor your social media platforms *Page 10*

Revise your policies and procedures regularly *Page 14*

Understand HIPAA

As a hospital marketing director, you've certainly been trained in HIPAA ad nauseam. But it's important to keep in mind the key elements of HIPAA.

The Health Insurance Portability and Accountability Act ([HIPAA](#)) is a federal [law](#) that says a patient has control of his or her own Protected Health Information, or PHI. No one else can release that information without consent of the patient.

The Health Information Technology for Economic and Clinical Health Act ([HITECH Act](#)) gives state attorneys general the right to enforce HIPAA as well.

A patient's PHI can be used for healthcare operations. It can be shared, for health care purposes, from a hospital to a physician, from a physician to a hospital, and to third party payors (insurance companies) and payment clearinghouses. But this information cannot be released beyond that circle without the consent of the patient.

KEY POINT: The rules regarding patient privacy that apply to everything else you do in healthcare also apply to social media activities. Remember that even the fact that the patient/doctor relationship exists is itself Protected Health Information.

CONSULT WITH YOUR LEGAL ADVISERS ***EARLY AND OFTEN***

This ebook is not meant to provide legal advice — just guidelines for implementing a HIPAA-compliant social media strategy. Seek legal advice for your particular hospital.

Limit liability by establishing clear policies and procedures

Determine a coherent set of internal and external policies and procedures regarding patient privacy that are tailored to your hospital.

Involve leaders, evangelists and frontline staff in the development of these policies and procedures. These policies should:

- 1 Explain appropriate use of social media platforms.*
- 2 Clearly define how information posted there will be used.*
- 3 Specify what degree of privacy can be expected.*
- 4 State clearly that these forums are not to be used for personal medical advice.*
- 5 State clearly that the site is NOT monitored 24 hours a day, seven days a week.*

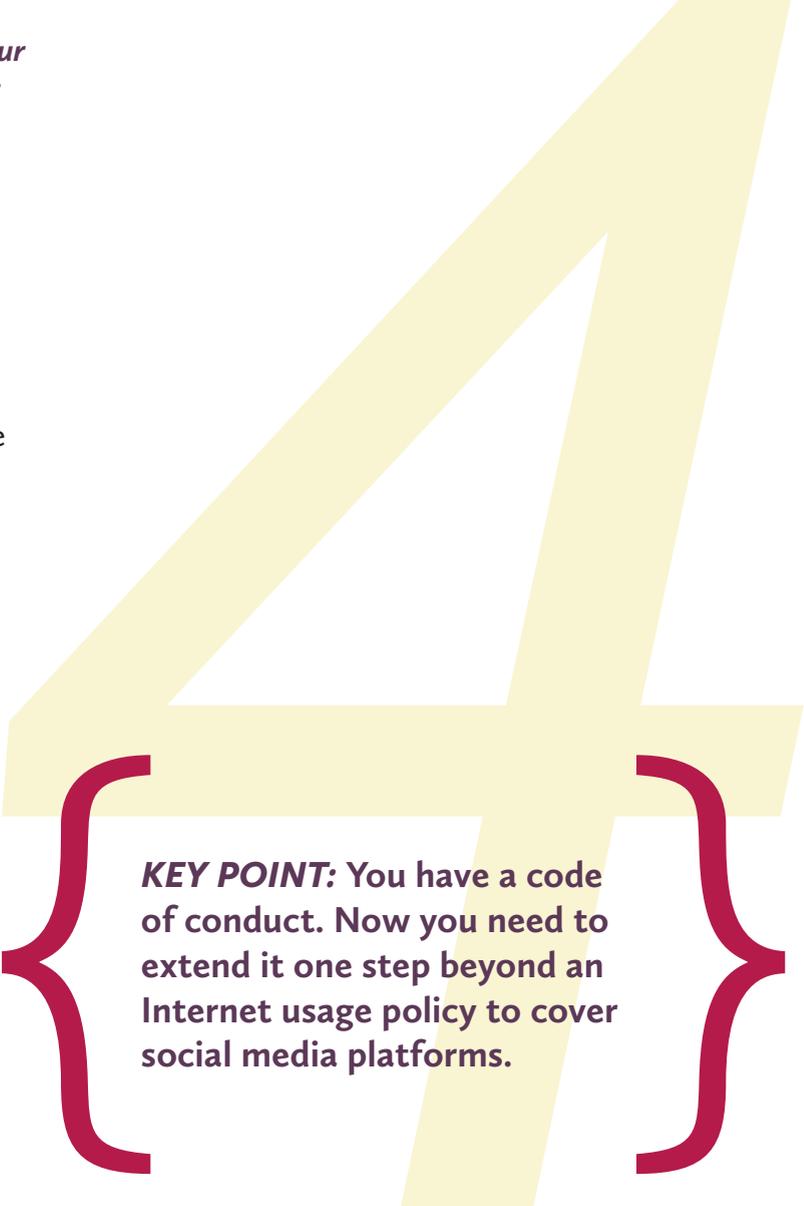
Post these policies prominently on your social media sites and incorporate them into off-line documents such as your Notice of Privacy Practices.



Train your staff in policies and procedures

Make sure all employees participating in your social media efforts have been trained, that they clearly understand your policies and procedures, and that they follow them.

Ed Bennett, who manages web and social media for the University of Maryland Medical Center, curates a large collection of [policies](#) on his website, Found in Cache. These are great to use as a point of reference, a starting point; policies must be developed locally so that they reflect local realities — including readiness to adopt social media — and achieve buy-in from affected personnel.



KEY POINT: You have a code of conduct. Now you need to extend it one step beyond an Internet usage policy to cover social media platforms.

Do not practice medicine online

While it is possible to conduct a hospital-patient relationship online, best practice would be to initiate the relationship in real life and obtain appropriate authorization from the patient to continue the dialogue online. Even then, don't practice medicine online in an unsecured social media environment. Many hospitals and their affiliated physician practices are developing patient portals to allow for more secure communication.

Some patients are more open than others and are willing to post details about themselves that others consider private. If someone posts these details in a public forum (e.g., “I’m cancer-free two years post treatment!”), that posting constitutes consent to the disclosure itself. Your response, however, should never disclose protected health information or offer tailored medical advice. The best approach is to respond publicly with a generic statement (“Great! Check out our XYZ Cancer Center of Excellence online at ...”), and reply privately as may be appropriate.

Take conversations offline.....

When you feel that comments or questions on your social media platform are approaching HIPAA violations, take conversations offline.

Ask the patient to call your hospital for more details. If issues come to your attention via social media — for example, tweets from your emergency room complaining about excessive wait time — deal with the issues offline, but report back to the online community about their resolution.

Transparency is a key feature of social media that can thrive even in the face of regulations such as HIPAA.



PROMINENTLY POST YOUR POLICIES AND PROCEDURES ON ***SOCIAL MEDIA PLATFORMS***

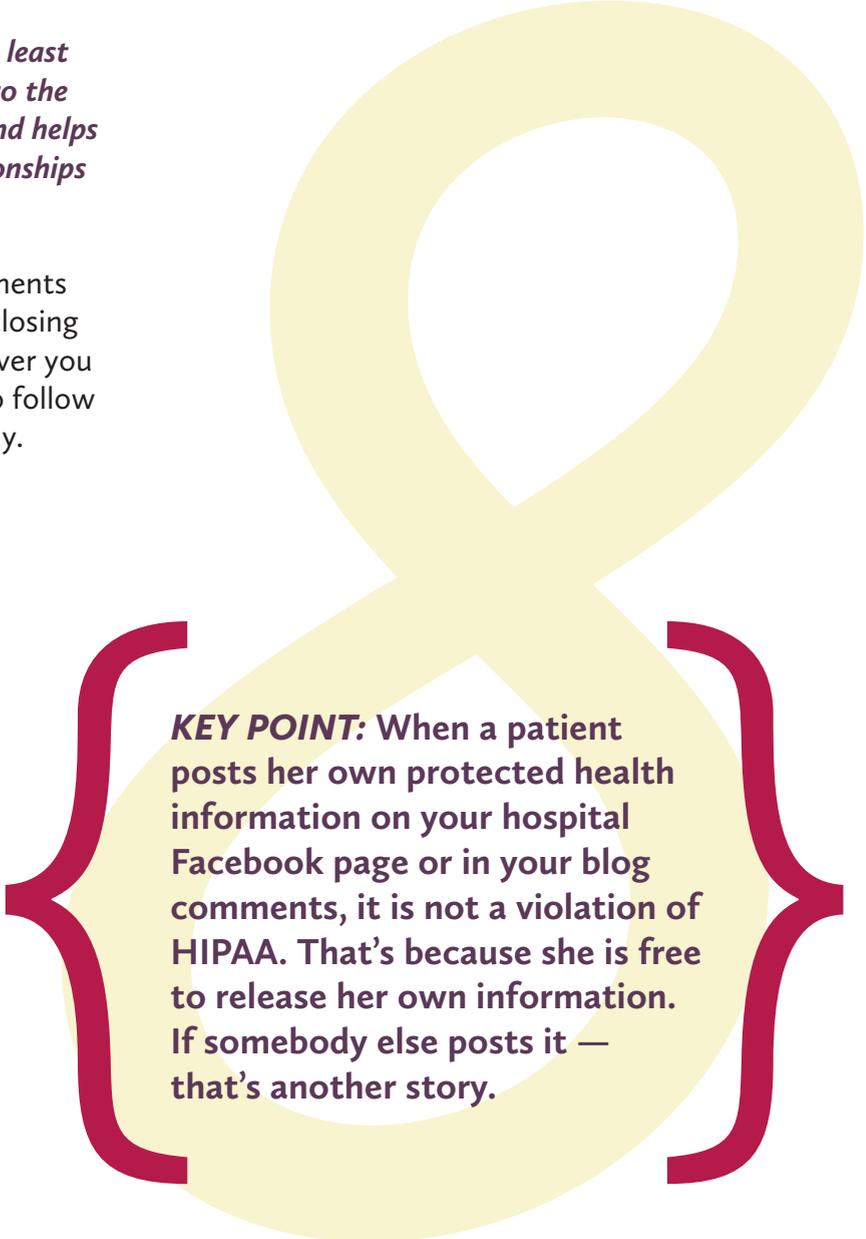
For instance, on Facebook have a separate tab for policies. On your blog posts, place a policies link just before your comments section. You can link to policies from Twitter profiles, too.

Make sure patients understand your policies and know how your hospital will interact with them. When you include prominent disclaimers and plenty of warnings, patients can make more informed choices about whether to disclose their own health information.

Regularly monitor your social media platforms

Review your social media platforms at least daily. That helps you respond quickly to the good and bad that comes your way, and helps you build those strong, trusting relationships that can be so powerful.

You should remove any posts or comments that violate HIPAA regulations by disclosing protected health information. Whenever you remove a comment or post, be sure to follow best practices by briefly explaining why.



KEY POINT: When a patient posts her own protected health information on your hospital Facebook page or in your blog comments, it is not a violation of HIPAA. That's because she is free to release her own information. If somebody else posts it — that's another story.

SOME IMPORTANT *QUESTIONS*

“Is our hospital liable for non-employee postings on forums we host?”

Andrea White, a senior account supervisor who is a specialist in health policy implementation at Lovell Communications in Nashville, Tennessee, writes that Section 230 of the Communications Decency Act “protects you as a sponsor of an online forum. A healthcare provider cannot be held liable for postings made by other parties just because it owns or sponsors the forum.”

We do have an additional caution, however. This law may help if you’re being sued for lewdness or slander, but in the healthcare privacy realm we’re held subject to a different set of standards. There are numerous overlapping state and federal regulatory schemas that apply to health care social media. Simply shrugging one’s shoulders and saying “I just set up the Facebook page, I didn’t write the post” will not absolve you of liability under health care privacy laws.

It becomes important to be able to monitor and potentially take down information if it reveals private information protected by HIPAA. Even if you’re not able to take down the offending post right away, if you have a schedule of scanning and scrubbing on a daily basis, that policy will work in your favor should an individual or a government agency register a complaint.

“Can we remove posts?”

Yes, according to White, with one important caveat. “You can take down or leave up comments as you deem... However, if you edit a third party’s post then you become the co-

author and assume liability. The moral is that you need to either respond to a comment, delete it, or leave it as it is. But NEVER edit it.”

“What liability do we have if we invite participation in a forum?”

White adds another caution: “If you want to invite new moms to post baby photos or ask weight loss program participants to track their results in a support group forum, then make sure

you have a terms of use policy [that they accept as a condition of participating in the forum] where they are voluntarily giving you permission to publish that information.”

“Are we liable for postings by a patient’s family or friends?”

No, says John Cummins, Health Leaders Media editor. He [writes](#), “I asked the Department of Health and Human Services’ Office of Civil Rights. They replied: ‘Entities subject to the HIPAA Privacy and Security Rules are covered entities: health plans, healthcare providers, and healthcare clearinghouses. Generally speaking, a covered entity would not be responsible for the actions by a patient’s friends or family.’”

However, in a forum that’s hospital-branded, the best practice is to ensure friends and family are not divulging protected health information of a patient, and even to reach out offline to friends and family who post any such information. As online tools evolve, it becomes easier to moderate content of forums, even Facebook pages.

“What if patients post photos they take in the hospital on social media sites?”

No problem, IF you post signage saying that picture taking is not permitted. John C. Parmigiani, president of John C. Parmigiani & Associates, LLC, and a nationally recognized expert in HIPAA compliance, [advises hospitals](#) to post signs at entrances to the emergency department or near emergency department examining rooms stating that picture taking is not permitted. That way, if a visitor ignores the rules, takes a picture and posts it online, the hospital can at least demonstrate that it was exercising reasonable measures to protect patient privacy.

“To me, the posting prohibiting picture taking would represent another example/level of ‘due diligence’ on the part of the hospital,” Parmigiani says.

Kate Borten, CISSP, CISM, concurs. Borten is president of [The Marblehead Group](#), a firm that provides information security and privacy consulting for the healthcare industry. Borten [explains](#) that HIPAA expects healthcare providers to take “reasonable” measures to protect patient privacy, but also “accepts situations such as waiting rooms where patients can be seen by the public or a family member accompanying a patient to a bed in the ER. As long as the hospital wasn’t doing something out of the norm, then it shouldn’t have any liability when a member of the public snaps a picture.”

Borten casts additional light on hospital’s responsibilities. HIPAA makes an “absolute distinction” between a

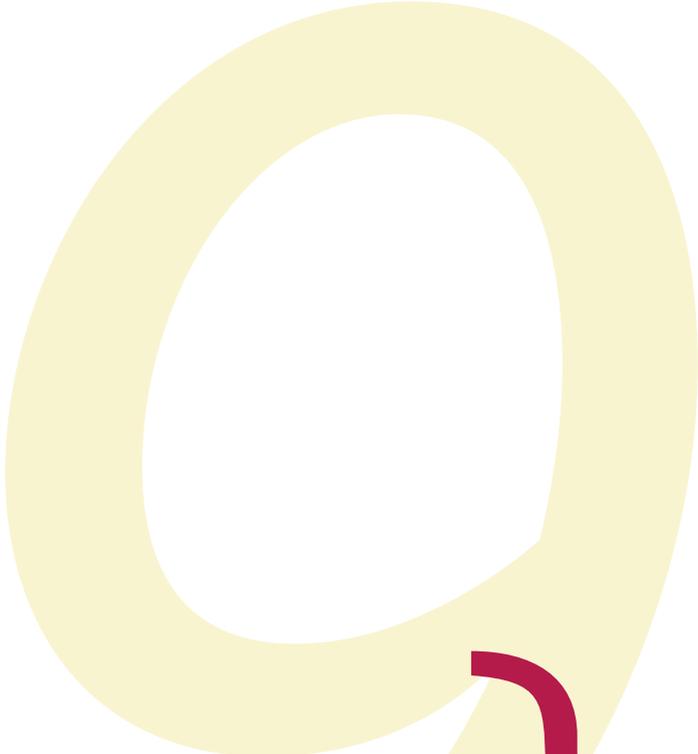
hospital’s workforce (defined in the regulations) and everybody else. “Organizations are responsible for the actions of their workforce, but not for the rest of the world,” Borten says.

Keep in mind, however, that a photograph taken of a procedure or other encounter gone wrong could end up in evidence in litigation against a hospital or its physicians. Furthermore, an inappropriate photo posted online in spite of a well-crafted no photography policy may generate negative publicity and could lead to lawsuits. In litigation over cases like these, even if you win, you lose. For these reasons, among others, mere posting of a policy prohibiting photography may not be enough.

Visit and revise your policies and procedures regularly

As social media evolves, as information technology becomes more pervasive, as you gain more experience and as your comfort level grows, you will need to revise and update your policies and procedures. Plan to review them at least annually.

Follow these steps and you should steer clear of HIPAA violations. Remember to contact your legal, compliance and human resources departments to make sure that your policies and procedures take all relevant laws and regulations into account, and are integrated with your institution's compliance and HR policies as well.



KEY POINT: HIPAA is an important touchstone to remember as you develop and implement your social media program, but just as important is the integration with the rest of your organization's policies and procedures.

The Authors

DAVID HARLOW is Principal of The Harlow Group LLC, a health care law and consulting firm based in Boston, MA. His twenty years' experience in the public and private sectors affords him a unique perspective on legal, policy and business issues facing the health care community.

David is adept at assisting clients around the country in developing new paradigms for their business organizations, relationships and processes so as to maximize the realization of organizational goals in a highly regulated environment, in realms ranging from facilities development to social media strategies to the avoidance of fraud and abuse.

His award-winning blog, HealthBlawg, is highly regarded in both the legal and health policy blogging worlds. He speaks regularly before health care and legal industry

groups on a broad range of topics, including the uses of social media. David is a charter member of the Advisory Board to the Mayo Clinic Center for Social Media. Follow him on Twitter.

David Harlow JD MPH

Principal

The Harlow Group LLC

Web: <http://harlowgroup.net>

Blog: <http://healthblawg.com>

*Twitter: @healthblawg
david@harlowgroup.net*

617.965.9732

DAN HINMON is principal at Hive Strategies, a firm that helps hospitals engage patients through social media.

Dan has been working in advertising, marketing and public relations since 1975. For 22 years he was president of Hinmon Agency, a full service advertising, marketing, public relations and design firm that served a variety of clients,

including hospitals, physician clinics, and health plans. In 2010 Dan founded Hive Strategies to help hospitals engage patients through social media.

With a bachelor's degree in political science and a strong ability to listen and communicate, Dan has a lifetime of experience helping clients connect with customers.

Dan Hinmon

Principal

Hive Strategies

Web: www.HiveStrategies.com

Blog: www.hivestrategies.com/social-media-strategy-blog/

Twitter: @hivedan

dan@hivestrategies.com

503.472.5512

