STRATEGIC MANAGEMENT SERVICES

Tips For Social Media Compliance

Richard P. Kusserow | August 2023

Key Points:

- **Social Media is a compliance "Danger Zone" for organizations and individuals**
- **Disclosures of PHI via social media are one of the common HIPAA violations**
- **Improper disclosures may implicate HIPAA as well as the Federal Trade Commission Act**
- **Most violations result from employees improperly social sharing**

There are many benefits to be gained from healthcare organizations using social media, such as raising awareness of emerging health issues, promoting healthy lifestyles, and making announcements concerning the availability of services. Health plans often use social media to market health insurance products, post profiles of staff, advertise new plans and benefits, and attract new customers. However, all of these uses of social media may be subject to FTC and HIPAA social media rules. HIPAA applies even though the law did not *explicitly* address social media because it was enacted years before social media networks existed (e.g., Facebook and Instagram). Both organization and personal use of social media can give rise to violation. According to the OCR, most HIPAA compliance violations occur from employees mishandling PHI, many of which stem from inappropriate social sharing. In many cases, posts by employees are innocent without improper intent. Violations are common because social media channels are easy for users who can take a photo, copy information, or make a comment that can be posted with a couple of clicks on the screen. It is simple for someone to post something with protected information on the Internet with little effort or thought. This requires everyone to separate their work and private lives and not to comment or post photos about work. Common examples of violations of HIPAA on Social Media include:

- Creating custom audiences for social ads
- Communicating through messaging platforms was permissible during the Pandemic but not now
- Posting patient information without written authorization

- Posting a picture or video of a patient in the foreground or background
- Reporting an athlete or celebrity injury
- Private messaging to colleagues regarding patients
- Posting patient information
- Responding to complaints or negative reviews, including patient information
- Neglecting to inform patients of any privacy breaches
- Sharing patient information with an agency
- Posting verbal "gossip" about a patient to unauthorized individuals
- Mistakenly believing posts are private or deleted when they are still visible to the public
- Sharing seemingly innocent comments that can be overheard or pictures visible patients

Violations under the HIPAA Privacy Rule include Civil Money Penalties, which can result in fines ranging from $100 – $1,500,000, or Criminal Penalties, which can result in fines up to $250,000 and up to 10 years in prison. Other consequences of violating HIPAA include lawsuits, losing a medical license, or employee termination.

20 Compliance Tips for Social Media

1. Ensure a full understanding of what is considered a HIPAA violation on social networks
2. Establish social media "rules" relating to permissible use and disclosures of PHI
3. Adopt social media HIPAA policies and procedures and train employees to follow them
4. Implement clear social media guidance regarding postings on social media
5. Establish related policies (e.g., Workstation Security, Bring Your Own Device (BYOD), etc.)
6. Make clear that seeking patient information via social media may violate HIPAA
7. Ensure easy access to written social media guidance, such as posting guidance on the Intranet
8. Enforce tough sanctions on anyone who violates social media policy
9. Establish a process for developing, managing, and monitoring privacy procedures
10. Secure patient PHI is not readily available to unauthorized parties
11. Deliver training on how social media applies to HIPAA privacy
12. Limit access to social media accounts
13. Notify patients about their privacy rights and how you use their information
14. Have a HIPAA social media compliance expert approve content before social media posting
15. Establish a workflow system for approving postings on social media
16. Use of "de-identified" information can be shared on social media without violating HIPAA.
17. Perform a Security Risk Analysis (SRA)
18. Implement controls to monitor for hashtags and keywords relevant to your organization

19. Establish ongoing monitoring and auditing for social media compliance
20. Promptly respond to any incidents involving potential social media violations

Keep up-to-date with Strategic Management Services by following us on LinkedIn.

About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.