

Social Media and PHI: A Slippery Summer Slope



From big wins to small snapshots, social media is a powerful tool that allows us to highlight life events. Online posts, however, can accidentally reveal more than we realize. That's why it's important to use social media wisely. Responsible social media practices allow you to safely connect with others and share what matters most, while upholding our commitment to keeping sensitive data secure. Review these guidelines to ensure online sharing stays within the appropriate boundary lines.

Skip the Snapshots – Summer workdays may be full of moments worth celebrating, such as team accomplishments or festive events, but taking photos during this time can create serious risks.

Background identifiers like patient charts, computer screens, and company information can unintentionally expose PHI. It's crucial to avoid taking photos in patient care areas and always follow guidelines for camera and phone usage. Review Lifepoint's [Mobile Application Security Standard Policy](#) and [Mobile Device Security Standard Policy](#) for additional details on mobile device protocols.



Observe What's Overlooked – Removing names, cropping out faces, or adding filters may seem like a way to safely share moments on social media, but these edits don't guarantee privacy. A familiar uniform, visible room number, glimpses of patient charts, or even a causal caption gives away more than we intend. In healthcare, even the smallest clues can lead to someone recognizing a patient, colleague, or care situation, compromising what should stay secure.

That's why HIPAA protects *any information that could be used to identify someone*. The safest approach is to keep work related content out of videos and photos entirely unless proper authorization has been given. What happens on the job most likely doesn't belong on social media.



Share Safely – It's not just photos that can cross the line; words can as well. A statement such as *"What a wild day at work"* or *"So proud of the team and how they handled things today"* can still disclose sensitive details. These types of messages hint at staffing levels, patient volumes, care disruptions, and facility incidents, information that should remain safeguarded.

In a world where one post can spread in seconds, indirect comments can catch the attention of patients, families, or news outlets, raising questions that put our organization at risk. The most secure move is to celebrate team wins offline or through approved internal channels, like [Making Moments Matter](#), where context and privacy are protected.



Protect Your Professional Space – Your online presence is an extension of your reputation, both personally and professionally. What is shared on social media can reflect your role in the workplace. It's important to adjust your privacy settings within online platforms, avoid engaging in anything patient-related, and pause before posting content that might cause inappropriate overlap between personal and professional communities.



Let's all be mindful of what you post on social media, how it could be interpreted, and who can view what you share. By following these guidelines, we can all uphold the professional standards that safeguard sensitive patient information.

Social Media and PHI: A Slippery Summer Slope

Put Our Social Media Guidelines to Test

What may seem like a harmless social media post, if not carefully reviewed, could expose protected health information (PHI) through visual details or context clues, putting patient privacy at risk. Curious about what can happen when privacy precaution takes a back seat to summer sharing? Review these hypothetical scenarios to understand why caution is key when posting online:

Scenario #1

An employee posts a photo of a patient's medical records on social media, exposing sensitive health information. The post attracts public attention, leading to a formal privacy complaint and triggering a federal investigation, resulting in a regulatory fine of over two million dollars.

Scenario #2

A workforce member was terminated after posting videos on social media that appeared to joke about patient care. Although the content was intended to be humorous, it crossed professional boundaries and violated privacy expectations, leading to disciplinary action.

Scenario #3

A local resident posts about their loved one's experience at a care facility. An employee, wanting to clarify the situation, comments with specific details about the patient's care and treatment plan. While the intention may be to protect the facility's reputation, this comment unintentionally discloses sensitive patient information without consent, leading to a violation of privacy.

Which example do you think carried the highest risk? **Leave a comment with "#1," "#2," or "#3" on this month's Firstup posting and tell us why.**

Can you identify which social media posts are safe, and which can put PHI at risk of exposure?

