Discussion 4 Social Media

Discussion Topic:

Comment on how social media can compromise protected health information.
Suggest ways in which such compromises can be mitigated.

My Post:

Hello Class,

Social media is everywhere today, and it's hard to ignore and not be part of it. In the white-collar world, professionals are expected to be active on social media platforms such as LinkedIn, Facebook, or X, which function as virtual resumes or portfolio showcases. I use my personal Facebook to keep track of my distant family members and friends.
If we use social media for professional or personal reasons, it is very easy to accidentally share Protected Health Information (PHI). Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, PHI is defined as an individually identifiable health information, such as health plans, medical records, or any information relating to the past, present, or future physical or mental health of an individual (HHS, 2024).

PHI is often intentionally shared on Facebook, Instagram, TikTok, or X, for example:
- By, taking a quick selfie and capturing a patient or individual in the background, a name on a wristband, a face, a chart, a room number, or a whiteboard with diagnoses.
- Even if no name was used in a post, descriptive details like age, rare condition, date/time, location, or a unique event can allow others to figure out who it was, especially in a small community.
- Posting a screenshot or a screen recording of a schedule, message thread, or EHR screen can expose PHI in seconds.
- Discussing a patient's health condition privately in DMs and messaging features can be forgotten, forwarded, leaked, or stored in unsecured ways.
- Patients, friends, and family members may choose to post about their health condition, but this does not automatically mean that the information can be reposted.
- Phones/apps data can spillover, that is, a patient's health info accessed on personal devices rather than organization devices may fall outside HIPAA protection (HHS, 2024).

Various methods can be used to mitigate these compromises, such as:
- Implement for yourself or for your organization clear social media rules, and make time aside for training.
- Use a minimum necessary information access or shared mindset. This means adopting a mindset that limits and adds conditions on uses/disclosures without authorization. This can be translated to only access and share what you truly must for the job, and never for social media.
- Establish rules prohibiting the sharing of any image or enforcing limitations, such as that patient images or stories cannot be shared without proper written authorization.

- Use strong technical control, such as Disable lock-screen previews for messages. Use HIPAA-appropriate communication tools for patient-related messages (not regular DMs).
- Create a culture where people encourage people to pause before posting (think before acting)

Approaching social media as a public space full of strangers (not a safe place to share PHI), rather than as a friend's house or a coworker's safe space, is an essential mindset for safeguarding health information.
"Think before posting!"
-Alex

References:

HHS. (2024, September 27). *The HIPAA Privacy Rule*. U.S. Department of Health & Human Services, Office for Civil Rights. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html