Tip #30: Social Media Hygiene for Healthcare Organizations

The Risk: Healthcare communication continues to become more electronic, and while social media accounts tend toward a more casual communication style, healthcare providers must remain vigilant about the security of their platforms, as well as the message they convey to their patients and potential patients.

Social Media Hygiene is a set of practices and behaviors related to cleaning up and maintaining your digital presence, in terms of both security and the message your social media applications deliver to patients and potential patients.[1] Much in the same way as we wash our hands with soap and water regularly, it is also critical to follow those practices that will keep you and your virtual data well protected, and convey an appropriate message for your organization.

Recommendations:

Performing proper social media hygiene is a two-step process, the first of which is system hygiene:

1. Regularly update all electronic devices and applications as recommended

2. Use passwords that follow appropriate security protocols:
    - Longer passwords are more secure: eight or more characters is recommended
    - Passwords should include different characters: numbers, symbols, and at least one capital letter
    - Avoid recycling passwords
    - Do not use the same password for all devices/apps/accounts
    - Do not allow staff to share passwords

3. Review the organization of files stored on your devices:
    - Determine that you have the right information and applications on the right device
    - Define those files that are mobile, laptop, and PC-appropriate

4. Optimize factory settings:
    - Use default settings as appropriate
    - Know how to disable, lock, or erase information in the event of device theft

[1] https://www.cloverinfotech.com/blog/cybercrime-is-infectious-digital-hygiene-is-the-vaccine/

5. Use multifactor authentication (MFA) for logging into your social media accounts

6. When able, employ device encryption

7. Lock down who can see your posts/information

These steps are often cited as the best measures to employ for protection against cyberattacks. However, your cybersecurity must extend beyond your device to include the information that is attached to you and your practice.

Reviewing the information on your social media platforms is the profile hygiene portion and second step of this process:

1. Analyze your current media profiles to determine if there is anything that:
   - Must be immediately addressed or can wait for revisions
   - Is no longer current

2. Clean up your digital past:
   - Delete old photos and posts that are no longer relevant
   - Delete old and/or neglected social media accounts

3. Ensure that the privacy settings on your platforms remain up to date

4. Review your blog and website:
   - Ensure that all information remains relevant and accurate
   - Consider whether the message presented about your practice is as you intend
   - If links are embedded, test that they are still functional and appropriate to your message
   - Delete any stale/non-functioning links, and, if appropriate, replace with current information

Routinely performing social media hygiene can help protect your practice from security breaches, keep your social media sites informative, and improve patient satisfaction.