Social Media and HIPAA - Frequently Asked Questions (FAQs)

One-Page Do's and Don'ts for Workforce Members

Do's

- **Protect patient privacy at all times.** Treat social media like any other public communication.
- **Obtain written patient authorization** before sharing any protected health information (PHI) through social media.
- **Use patient authorization only for CUIMC purposes.** Authorization does not apply to personal or non-CUIMC uses, including personal accounts or websites.
- **Follow CUIMC Social Media and HIPAA policies** at all times.
- **Be cautious when taking photos or videos** in clinical or work areas—patient information may appear in the background.
- **Report potential HIPAA violations immediately** according to CUIMC procedures.
- **Complete required HIPAA and social media training** and stay familiar with updates to policies.

Don'ts

- **Do not post patient information on social media** without written authorization—even if:
  - The patient's name is not included
  - The patient posted first
  - The post is positive or intended to celebrate a success
- **Do not post photos or videos of patients** on any personal social media account or website.
- **Do not share images that may identify a patient indirectly**, such as:
  - Faces, tattoos, or unique features
  - Room numbers, charts, wristbands, or computer screens
- **Do not respond to patient comments or reviews** with any patient-specific information.
- **Do not assume content can be deleted or taken back.** Social media posts can be shared, saved, or screenshot.
- **Do not use CUIMC authorization forms for personal use.**
- **Do not connect with patients on personal or professional social media accounts.**

Remember

- HIPAA applies to disclosures of PHI on **all social media accounts**, including personal accounts.
- Even a single post can result in **discipline, termination, or fines**.
- When in doubt: **Don't post. Ask first.**