Tips for dealing with Social Media

Facebook

- Remove yourself from Facebook search results

- Avoid the "Infamous Photo/Video Tag Mistake"

- Protect your photo albums

- Prevent stories from showing up in your friends' news feeds

- Make your contact information private

- Avoid embarrassing wall posts

- Keep your friendships private

- Protect against published application stories

Blogs

- No identifiable patient information.

- No identifiable student/resident/fellow information

- Remember that previous posts can help identify your location and position.

- Consider blogging programs that allow you to lock your posts.

- Remember that anyone who reads the posts can cut and paste or get a screen capture

All Media

- Avoid posting anything that you would not want everyone to read

- Protect all passwords, logons and other access information. Do not use the same passwords for social media that you do for your work, business and other accounts.

- Occasionally "Google" yourself or your postings

- Learn the platform that you are using

- Do not use the same passwords for social media that you do for your work, business and other accounts.

- It is inappropriate to "friend" patients on any social networking site or to check patient profiles.

- Identifiable protected health information (PHI) should never be published on the internet

- Refrain from posting material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful or embarrassing to another person or any other entity.

- It is never appropriate to provide medical advice on a social networking site.

- Consider setting privacy at the highest level on all social networking sites.