Privacy/Security Risks Associated with Use of Social Media

Communicating with Us

Please do not send any private or confidential information to us by social media. We strongly urge you not to use social media for private/confidential messages, because **social media is not a secure means of communication**.

What is "unsecure" about social media?

Typically, messages sent through social media delivery systems (such as Facebook Messages, Facebook Chat and Twitter Direct Messages) travel across the Internet, passing through multiple computers before reaching their final destination. You cannot know whether a message you send will be viewed along the way. Similarly, the messages are stored on the social media application's servers unless you permanently delete them. If someone gets access to your account (for example, another family member who uses your computer), they could see the messages in this archive and posts or comments you have made. We urge you to only access the pages pertinent to this research on a private computer and to ensure you log-out after you are finished with your communication.

Each social media platform offers different default settings to protect privacy and confidentiality as well as different levels of user control over what content is shared to whom. Please review that information and the privacy settings carefully before commenting, posting, or sending a message. Once content is posted or sent, privacy and confidentiality cannot be assured.

There are many other ways in which social media are not secure—these are only selected examples.

What should I do?

Do not hesitate to contact us by [insert approved research-related social media platform] for routine matters, such as asking for technical advice on how to use the platform. However, for communications that relate to private matters—such as diagnoses, symptoms, family relationships and so on—we urge you to call us at XXXXX so that we can have a private discussion regarding your questions/concerns.