Columbia University Irving Medical Center

Social Media and HIPAA

Frequently Asked Questions (FAQs)

1. What should you know about social media and HIPAA?

Posting protected health information (PHI) on social media is permissible under HIPAA **only** if you have written authorization from the patient. When patient authorization is obtained, it is only valid for CUIMC. Workforce members may not use CUIMC HIPAA Media Authorization for personal or non-CUIMC purposes.

2. Why does social media increase the risk for HIPAA violations?

Social media channels make it easy for users to take a photo or video and upload it with the tap of a screen. This increases the risk for HIPAA violations because workforce members can take a photo or video of something or someone they have seen and post it within seconds. If it reveals health information (for example, a computer screen with patient information in the photo), it is a violation of HIPAA unless the written authorization of the patient was obtained in advance.

3. What is considered a HIPAA violation with social media?

In general, workforce members posting any individually identifiable health information without a written authorization can be considered a HIPAA violation. If an authorization is obtained, the form on which the disclosure is authorized **must inform the patient what the disclosure is for and explain that the patient has the right to revoke the authorization**. The authorization should also include the option of stipulating a time after which the disclosure must end.

4. If an employee uploads a picture of a patient's injury to an Instagram reel without any other identifying information, is that a breach of the HIPAA Privacy Rule?

Yes, it is a breach of the HIPAA Privacy Rule if the identity of the individual can be determined from the image. However, please review the organization's CUIMC's Social Media policy.

5. Do the HIPAA social media rules apply to all accounts or just work accounts?

The HIPAA social media rules apply to **all accounts** – not just medical center accounts. It is important to be aware that images posted on personal social media accounts without patient

consent are in violation of HIPAA, as the individual has not only posted PHI impermissibly, but they have also used the image in violation of the organization's policy.

6. Do all employees have to be trained in HIPAA social media rules, or just those with access to ePHI?

All workforce members should be trained in HIPAA social media rules as part of their awareness training. Everyone should be aware of the organization's policies relating to social media whether they have access to PHI or not. Even members of the workforce without access to PHI can disclose information on social media such as a patient's name and what they are being treated for, so it is important we know not to disclose information without authorization through any media.

7. Why is posting patient information on social media a HIPAA violation?

Posting patient information on social media is a HIPAA violation if you do not have the patient's authorization because it discloses individually identifiable health information to the public. Even if you do not name the patient when you post protected health information (PHI) on social media, the patient can still be identified from other information included in the social media post.

8. How can healthcare organizations implement controls that flag potential HIPAA violations on social media?

Healthcare Organizations should implement controls that flag potential HIPAA violations on social media. For example, the simplest way for healthcare organizations to monitor social media for HIPAA violations is to search for specific hashtags relating to a healthcare facility (i.e., NYP, Columbia, CUIMC, etc.).

9. What is HIPAA compliant social media policy?

A HIPAA compliant social media policy stipulates the circumstances under which it is allowed to post any information to social media. As social media posts can never be fully retracted (because they may have been shared, screenshot, or copied and pasted prior to retraction), it is a best practice to prohibit any post containing individually identifiable health information unless patient authorization is obtained and sanction any member of the workforce that violates this policy.

10. What is the penalty for a social media HIPAA violation?

The penalty for a social media HIPAA violation depends on who is responsible for the impermissible disclosure of PHI and what are the consequences. For example, if an individual posts PHI on a social media site without authorization for a marketing campaign, and the subject(s) of the PHI complain to HHS Office for Civil Rights, the penalty could be a substantial fine. However, if a member of the workforce posts PHI on a social media site without authorization, the penalty could range from a verbal warning and retraining to termination.

11. Is Facebook HIPAA compliant?

Although Facebook has mechanisms to control unauthorized access to accounts, Meta will not sign a Business Associate Agreement with covered entities. Thus, **Facebook is not HIPAA compliant**.

12. Are there any examples of HIPAA violations on social media?

There are several examples of HIPAA violations on social media that have resulted in fines being issued by HHS Office for Civil Rights and dozens of examples of employees being fired and/or charged for HIPAA violations on social media.

- In 2017, ProPublica published more than fifty examples of HIPAA violations on social media that resulted in employees being sanctioned, fired, and/or charged with a criminal offense.
- In 2019, Elite Dental Associates was fined $10,000 for disclosing a patient's name, details of her health condition, treatment plan, insurance, and cost information in response to a negative online review.
- In 2022, another dental practice – Dr. U. Phillip Igbinadolor and Associates – responded to a patient complaint on social media disclosing the patient's name and treatment. The dentist was fined $50,000.
- In 2025, HHS OCR fined a rehab facility for $185,000 for posting over 150 patient success stories including the patient's name, photo and medical information on their organization's website without patient authorization.

13. What are the recommended social media guidelines for healthcare professionals?

The recommended social media guidelines for healthcare professionals is **not to post or respond to anything relating to patients on social media channels**. Even if the patient chose to post something positive about their care, that **does not** provide authorization to comment about someone you are caring for or have treated. Also, there is no way you can fully retract a social media post if the patient decides to revoke their authorization. Finally, if a friend or family member of the patient – who does not know you had the authority to publish the patient's PHI – sees the post, they may file a complaint with your employer or HHS Office for Civil Rights.

14. Is posting a photo of a patient on social media considered a disclosure?

Posting a photo of a patient on social media is considered a disclosure if the photo identifies the individual and either the photo or a description of the photo implies a past, present, or future treatment relationship. However, posting a photo of a patient on social media is not necessarily an impermissible disclosure if you have obtained the patient's written authorization. Again, CUIMC Social Media Policy prohibits personal use of patient information.

Note: In 2015, the California Board of Registered Nursing revoked an RN's nursing license after she shared images of a patient's surgical wounds on Instagram in violation of HIPAA. Although the patient was not named in the Instagram post, the images showed identifying tattoos and the patient's room number.

15. Is it a HIPAA violation to look up a patient on Facebook?

It is not a HIPAA violation to look up a patient on Facebook because information on Facebook is posted by individuals who are publishing information about themselves in the public domain. Workforce members are discouraged from connecting with patients on personal social media platforms.

16. Who is allowed to share personal health information on social media sites?

The issue of who is allowed to share personal information on social media sites is complicated. There are guidelines in HIPAA about sharing protected health information on social media, but if an individual or organization is not covered by the HIPAA guidelines or an employer's social media policy, other data privacy laws may apply – and these can vary from state to state.

17. What are the rules for social media and patient privacy in HIPAA?

There are no specific rules for social media and patient privacy in HIPAA because HIPAA was created many years before social media. However, organizations have social media policies that address workforce members posting patient information on social media channels and outline the procedures to post patient information on social media channels in compliance with HIPAA.