irwin siegel agency
INSURANCE PROGRAMS & RISK MANAGEMENT

SOCIAL MEDIA COMMENTS

A GUIDE FOR HOW TO RESPOND

A mental health center recently reached an agreement with the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) after they responded to an individual's negative online review using protected health information. The individual's diagnosis and treatment of their mental health condition were impermissibly disclosed when the organization posted a response to the negative online review.

HIPAA Privacy and Security rules prohibit the impermissible use or disclosure of patient-protected health information (PHI) as this breaches or violates the patient's privacy and security. As such, sharing too much information on social media platforms can cause avoidable consequences for businesses.

According to HHS, most HIPAA compliance violations from recent years have occurred from employees mishandling PHI, many of which stem from inappropriate social sharing. Violations under the HIPAA Privacy Rule include Civil Money Penalties which can result in fines ranging from $100 - $1,500,000 or Criminal Penalties which can result in fines up to $250,000 and up to 10 years in prison. Other consequences of violating HIPAA include lawsuits, the loss of a medical license, or employee termination. In 2022, a record-breaking 22 HIPAA enforcement actions were settled resulting in financial penalties over $2.1 million; 2023 has already seen 7 violations and $1.9 million in HIPAA fines as well.

HIPAA rules apply to all social media accounts – not just corporate accounts. It is important to be aware that images posted on private social media accounts without patient consent are in double violation of HIPAA, as the individual has not only posted ePHI impermissibly, they have also obtained the image from a corporate source that lacked the protections of the HIPAA Security Rule.

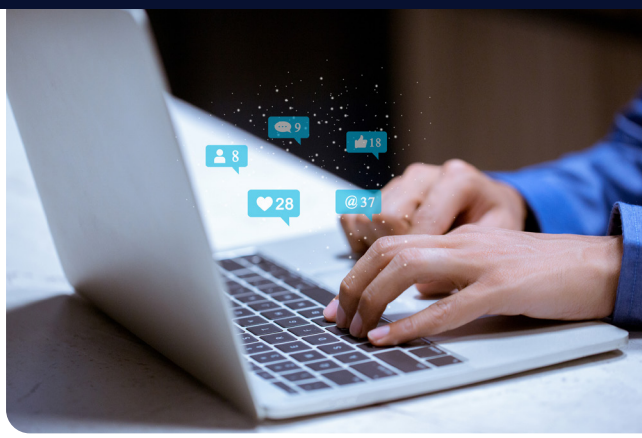
Common examples of social media HIPAA compliance violations include:

- Posting verbal "gossip" about a patient to unauthorized individuals, even if the name is not disclosed.
- Sharing of photographs, or any form of PHI without written consent from a patient.
- Sharing of seemingly innocent comments or pictures, such as a workplace lunch which happens to have visible patient files underneath.
- Responding to posts, comments, reviews, etc. regarding the organization while inadvertently disclosing private patient information

800.622.8272 | www.isa-risk.com | riskmanagement@siegelagency.com

irwin siegel agency
INSURANCE PROGRAMS & RISK MANAGEMENT

SOCIAL MEDIA COMMENTS
A GUIDE FOR HOW TO RESPOND



While it may seem harmless or convenient to respond to comments or feedback on social media platforms, situations can quickly escalate. Here are a few risk management recommendations when responding to online comments:

- Designate a specific individual in the organization whose job includes monitoring social media posts.
- Review posts frequently and respond promptly to positive and negative comments. Responding to each review – positive and negative – helps the overall reputation of the organization.
- Keep the responses short and simple
  - Thanks (name). We appreciate your comments.
- If the comments are negative, acknowledge the comment and reach out to request additional information
  - We would like to speak with you directly to discuss your concerns. Please contact (name and title) at (phone number) so we can work together to resolve your concern.
- Avoid going back and forth with the individual when responding online. If the individual continues to make comments, add one additional statement such as:
  - Because of privacy laws, we are unable to respond to the specifics regarding your care online. We care about your comments and would like to speak with you directly. Please contact (name and title) at (phone number) so we can work together to resolve your concern.
- Establish a system to identify concerns which may warrant further review. Are there issues which should be referred to Risk Management or Peer Review for further discussion? Sometimes an individual's complaint is the first notice of a potential legal issue. This information may also be used to develop trends and concerns for quality or performance improvement projects.

It is equally important to integrate your organization's social media policy with your organization's HIPAA Privacy and Security policies and procedures and train employees on them at hire and at least annually afterwards.

Remember that a HIPAA compliance program is ongoing and ever changing, so vigilance is key and must be part of your overall program. By providing ongoing training to employees regarding potentially hazardous mistakes while using social media and medical blogs, your organization will ensure social media is a powerful tool for sharing information, sharing experiences, and potentially expanding your organization's business.