

Clinical Communications and Privacy

Ronald Schouten, MD, JD, CTM, DLFAPA

Director, Forensic Psychiatry Fellowship Program

Saint Elizabeths Hospital

Washington, DC

Affiliate Professor of Psychiatry & Behavioral Sciences

Howard University College of Medicine

Department of Psychiatry, Massachusetts General Hospital

Disclosures

Neither I nor my spouse/partner has a relevant financial relationship with a commercial interest to disclose.

Case example

Dr. Smith finished residency in 2022. Due to the pandemic, her practice was primarily virtual starting in March 2020. Dr. Smith is an active user of TikTok, Instagram, and other social media. Like others in her age group, Dr. Smith communicates primarily by text rather than by telephone.

Following graduation from residency, Dr. Smith took a part-time job with the hospital where she did her training. As part of that job, she has an encrypted email account. She also starts an outpatient clinical practice. Tuned into current social media marketing trends, she sets up a LinkedIn account, an Instagram page linked to her practice, and a webpage <http://www.DrSmithCares.com>, along with an email address: DrSmith@DrSmithCares.com. Still paying off her medical school loans and with limited cash reserves, she uses her personal cell phone number for her practice. Through her LinkedIn, Instagram, and webpage, she cultivates an image of being open, warm, and welcoming, and in touch with current cultural and political trends. In other words, she offers a cool, caring vibe.

Shortly after opening her private practice. Dr. Smith receives a text message: “Hey, Dr. S., I saw your Instagram and web page and I think you are the right therapist for me. I was abused by my parents and have lots of issues related to childhood trauma, including an eating disorder and relationship problems. I could really use your help and hope we can connect. Please text me at 617 xxx-xxxx or email me: Sarah@sarah.com

Dr. Smith responds to the text message via email “Hi, Sarah. I’d be happy to see you this Monday at my private office (address on the website) at 10:00. Will that work for you? If so, please fill out the attached form and email it back to me.” The pdf form she attaches is a comprehensive questionnaire covering social, psychiatric, medical, and family histories and symptoms and chief complaint.

Dr. Smith confirms receipt of the form via text message, inadvertently addressing it to another patient.

Any problems here?

HIPAA: Health Insurance Portability and Accountability Act

- Primary purposes
 - Ensure portability of health insurance when changing employers
 - Prevent unauthorized disclosures of medical information
 - Facilitate the exchange of medical information to improve the efficiency of care
- Civil and criminal penalties
- Pre-empted by more protective state law (including privacy/social media)
- HIPAA pre-dates social media and the digital world
- No unauthorized disclosure of PHI except in the public good

Protected Health Information (PHI) Under the Privacy Rule

- Identifying information
 - Name
 - Address
 - SSN
- Past, present, or future condition
 - Mental
 - Physical
- Services/ treatment provided
- Payment

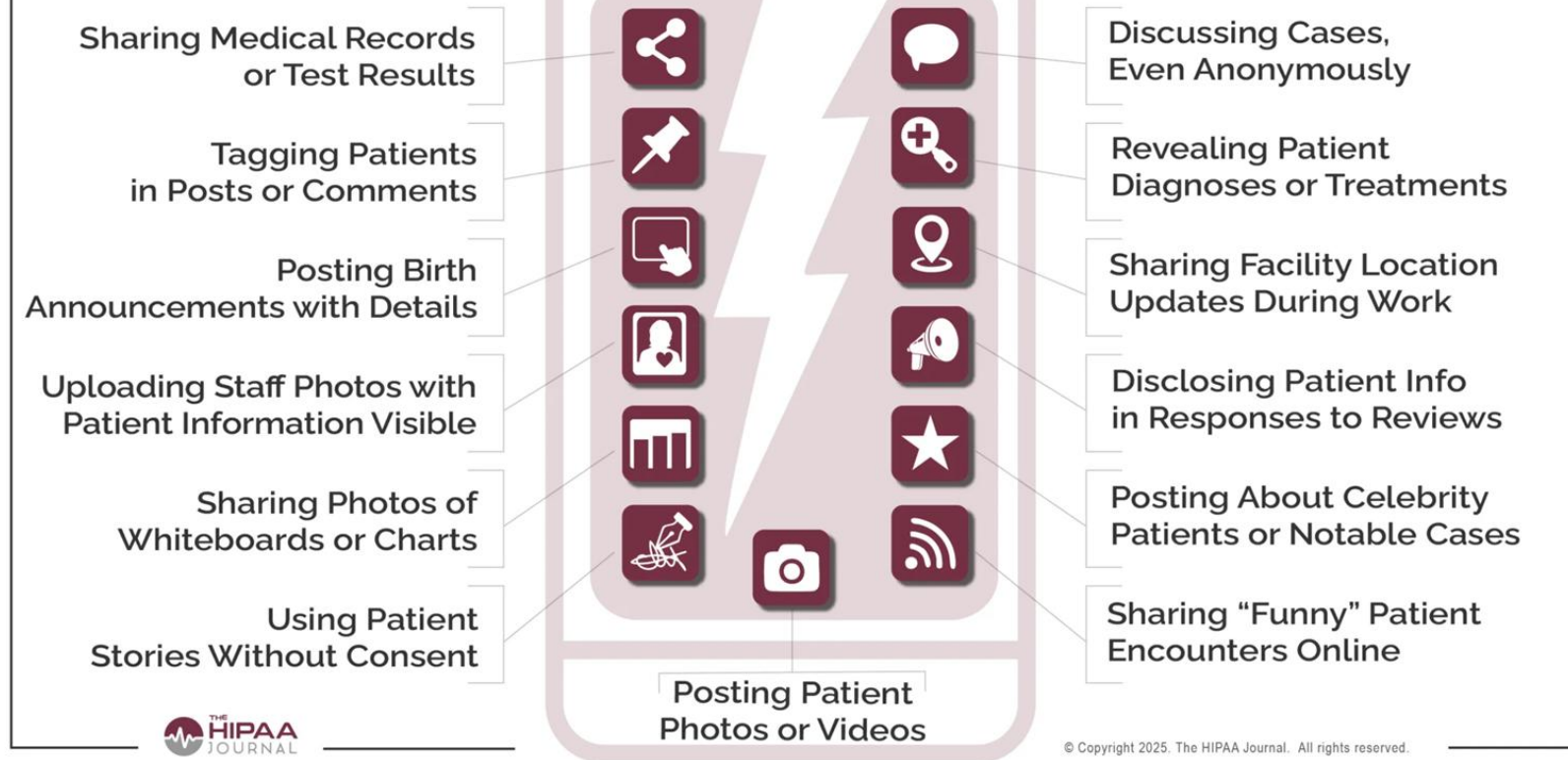
How MHPs can get in trouble with digital communications

- Sending PHI via standard email platforms without a Business Associate Agreement (binds vendor to protecting privacy of PHI)
- Unsecured messaging platforms
 - SMS and MMS are least secure-can be read by a third party with network access; temporarily stored on carrier's servers; susceptible to hacks
- Unsecured video conferencing platforms (e.g., standard FaceTime or Zoom)

How MHPs can get in trouble with digital communications

- Discussing PHI on social media
 - Commenting on a case, even if anonymous
 - Acknowledgment of role in a patient's care
- Sharing PHI outside of “treatment, payment, and operations” (e.g., with family) unless it is an emergency
- Failure to maintain audit logs
- Penalties for ePHI HIPAA violations
 - Fine imposed on the practice entity
 - Individual employee: verbal warning/retraining termination/loss of license
- Risks of communication via text messages
 - Unencrypted can be hacked/read by others
 - Sending error
 - Losing track of information (e.g., dosage, instructions)

HIPAA Violations on Social Media



<https://www.hipaajournal.com/hipaa-social-media/>

Staying out of trouble with e-PHI

- Informed consent for electronic communication
 - To communicate via text/email
 - Warning regarding limitations on security/privacy
- Pt initiated email contact:
 - Per HHS OCR (2008): can assume communication by email is acceptable to patient. But.
 - States have passed laws requiring confirmation of that consent: Connecticut, Colorado, Texas, Tennessee, Virginia, Utah, Montana, Iowa, and Indiana (from January 2026)
- Use HIPAA-compliant platforms
 - Encrypted websites (https://)
 - Encrypted email not required by HIPAA—but a good idea
 - “Send secure” email for those sent outside your organization
 - Encrypted messaging apps:
 - “Signal”
 - “What’s App”
 - “Telegram”
 - Patient portals

Staying out of trouble with texting

- End-to-end encrypted apps (E2EE):
 - Examples: Signal, WhatsApp, Threema.
 - Most secure.
- Mixed-encryption apps:
 - Examples: iMessage, Telegram
 - Security level varies
 - iMessage uses E2EE only when communicating between Apple devices
 - Telegram uses E2EE if manually enable and only for one-to-one messaging
- Ephemeral messaging apps
 - Examples: Snapchat, Wickr)
 - Messages are automatically deleted after viewing or a set period of time
 - Security level varies
- Business and enterprise messaging platforms
 - Examples: Slack, Microsoft Teams
 - Primarily for workplace collaboration
 - Security level depends upon how the organization sets the level

Staying out of trouble

- Implement security controls
- No posting on social media without express patient authorization
 - Case descriptions (even if anonymous)
 - Photographs from which patient may be identifiable
- Do not respond to “Yelp” reviews with PHI (including acknowledging care)
- Establish a social media policy for your practice
 - Training
 - Sanctions
- Follow the minimum necessary rule



HIPAA Privacy Rule and Sharing Information Related to Mental Health

Background

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides consumers with important privacy rights and protections with respect to their health information, including important controls over how their health information is used and disclosed by health plans and health care providers. Ensuring strong privacy protections is critical to maintaining individuals' trust in their health care providers and willingness to obtain needed health care services, and these protections are especially important where very sensitive information is concerned, such as mental health information. At the same time, the Privacy Rule recognizes circumstances arise where health information may need to be shared to ensure the patient receives the best treatment and for other important purposes, such as for the health and safety of the patient or others. The Rule is carefully balanced to allow uses and disclosures of information—including mental health information—for treatment and these other purposes with appropriate protections.

In this guidance, we address some of the more frequently asked questions about when it is appropriate under the Privacy Rule for a health care provider to share the protected health information of a patient who is being treated for a mental health condition. We clarify when HIPAA permits health care providers to:

- ✓ Communicate with a patient's family members, friends, or others involved in the patient's care;
- ✓ Communicate with family members when the patient is an adult;
- ✓ Communicate with the parent of a patient who is a minor;
- ✓ Consider the patient's capacity to agree or object to the sharing of their information;
- ✓ Involve a patient's family members, friends, or others in dealing with patient failures to adhere to medication or other therapy;
- ✓ Listen to family members about their loved ones receiving mental health treatment;
- ✓ Communicate with family members, law enforcement, or others when the patient presents a serious and imminent threat of harm to self or others; and
- ✓ Communicate to law enforcement about the release of a patient brought in for an emergency psychiatric hold.

In addition, the guidance provides relevant reminders about related issues, such as the heightened protections afforded to psychotherapy notes by the Privacy Rule, a parent's right to access the protected health information of a minor child as the child's personal representative, the potential applicability of Federal alcohol and drug abuse confidentiality regulations or state laws that may provide more stringent protections for the information than HIPAA, and the intersection of HIPAA and FERPA in a school setting.