## Protecting Patient Privacy in the Digital Age: A Guide for Mental Health and Rehabilitation Center Staff

# What is Protected Health Information (PHI)?

Protected Health Information includes all individually identifiable health information that is created, received, maintained, or transmitted electronically (Isola & Al Khalili, 2023). This includes:

- · Patient names, addresses, and dates
- Medical record numbers
- Photos and images
- Treatment information
- Payment information
- · Any other unique identifying characteristics

### Social Media Best Practices & Risk Mitigation

#### **Never:**

- Post any patient information or photos
- Discuss cases, even without names
- · Share facility locations or identify patients
- · Take photos in treatment areas

#### **Always:**

- Use separate personal and professional accounts
- Review privacy settings regularly
- Report breaches immediately
- Consider how posts might identify patients indirectly (Galea et al., 2023)

Privacy, Security, and Confidentiality in Healthcare Technology

#### Privacy:

Patients' right to control their health information

- Example: Obtaining patient consent before sharing information
- Critical in mental health settings due to stigma and sensitivity

#### Security:

Technical safeguards protecting PHI

- Encrypted devices and secure networks
- Two-factor authentication
- Regular security updates
- Secure password practices

#### **Confidentiality:**

Obligation to protect patient information

- Information shared only with authorized personnel
- Need-to-know basis for accessing records
- Special consideration for mental health and substance abuse information (Shojaei et al., 2024)





## Consequences of Social Media Violations

- Nurse contract termination for sharing patient information
- HIPAA fines for healthcare organizations
- Loss of professional licenses
- Criminal charges for severe privacy violations

### Interdisciplinary Team Responsibilities

- ALL team members are responsible for PHI protection
- Report concerns to Privacy Officer immediately
- · Regular training participation required
- Collaborate to maintain secure communication channels
- Support colleagues in maintaining compliance

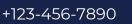


## Steps if a Breach Occurs

- Immediately document the incident
- Report to Privacy Officer
- Do not delete evidence
- Cooperate with investigation
- Participate in corrective action

### Evidence-Based Prevention Strategies

- Regular staff training (reduces breaches by 40%)
- Clear social media policies (reduces violations by 65%)
- Automated monitoring systems
- Immediate breach reporting protocols
- Team-based accountability systems (Galea et al., 2023)





#### References

- **1.**Galea, G., Chugh, R., & Luck, J. (2023). Why should we care about social media codes of conduct in healthcare organizations? A systematic literature review. Journal of Public Health, 32(2), 1–13. https://doi.org/10.1007/s10389-023-01894-5
- **2.** Isola, S., & Al Khalili, Y. (2023). Protected health information. PubMed; StatPearls Publishing. https://www.ncbi.nlm.nih.gov/books/NBK553131/
- **3.** Shojaei, P., Gjorgievska, E. V., & Chow, Y.-W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. Computers, 13(2), 41. https://doi.org/10.3390/computers13020041