[Company Name] Healthcare Employee Social Media Policy Template

A practical, editable policy template for hospitals, clinics, health systems, medical groups, pharmacies, insurers, and other healthcare organizations.

> **Template note**
> This document is a general workplace policy template. It should be reviewed by legal, HR, privacy, compliance, and security teams before use. Replace all bracketed placeholders with organization-specific details.

Prepared for	[Company Name]
Version	[Version Number]
Effective date	[Effective Date]
Owner	[Department or Role]

Table of Contents

1. Purpose

[Company Name] recognizes that employees use social media to communicate, learn, network, and share personal experiences.

This policy explains how employees should use social media when their activity may relate to [Company Name], our patients, members, clients, residents, coworkers, providers, facilities, services, business partners, or reputation.

The goal is not to control every personal post. The goal is to protect patient privacy, preserve trust, prevent unauthorized disclosures, reduce legal and compliance risk, and help employees understand how workplace expectations apply online.

2. Who This Policy Applies To

This policy applies to all [Company Name] workforce members, including:

- Full-time and part-time employees
- Temporary employees
- Clinical and administrative staff
- Remote and hybrid employees
- Providers and clinicians employed by [Company Name]
- Managers and supervisors
- Interns, students, residents, and trainees
- Contractors, consultants, vendors, and agency workers acting on behalf of [Company Name]
- This policy applies to personal social media use when posts relate to [Company Name], patients, members, coworkers, facilities, healthcare services, company information, or work-related matters.

3. Platforms Covered by This Policy

This policy applies to social media platforms, messaging apps, forums, review sites, video platforms, blogs, livestreams, online communities, private groups, and public comment sections.

- Facebook, Instagram, TikTok, X, LinkedIn, Reddit, YouTube, Snapchat, Threads, Discord, WhatsApp, Slack, Microsoft Teams, blogs, forums, review sites, private groups, and any future platform where users post, comment, share, message, record, stream, or upload content.
- Private accounts, restricted groups, disappearing messages, or friends-only settings do not guarantee privacy. Screenshots, reposts, recordings, forwarded messages, and archives can still exist after the original post is deleted.

4. Personal Accounts vs. Official Company Accounts

Employees may use personal social media accounts for personal expression. However, employees should make clear when they are speaking for themselves and not for [Company Name].

Only authorized employees may post from official [Company Name] accounts or speak publicly on behalf of [Company Name].

Employees may not create accounts, pages, groups, usernames, or profiles that appear to represent [Company Name], a facility, a department, a service line, or a care team unless approved by [Department or Role].

Employees may not use [Company Name] logos, trademarks, facility names, uniforms, internal images, patient care areas, or brand assets in a way that suggests official approval unless authorized.

5. Patient Privacy and Protected Health Information

Employees must never post, share, upload, record, livestream, screenshot, forward, or disclose protected health information or any patient-identifying information on social media.

> **High-risk area**
>
> Do not post patient details, photos, videos, stories, or screenshots unless the required approval and written authorization are in place.

- Patient names, faces or images, dates of birth, medical record numbers, addresses, phone numbers, email addresses, insurance information, appointment details, test results, diagnoses, treatment details, medication information, billing information, photos or videos from patient care settings, and stories or situations that could allow a patient to be identified.
- Employees should not discuss patient situations online, even if the patient's name is not included, if the patient could reasonably be identified from the details.
- Employees may not post patient photos, patient videos, patient stories, or patient testimonials unless approved through [Department or Role] and supported by the required written authorization.

6. Respect Patients, Families, Members, and Caregivers

Employees may not use social media to mock, shame, insult, expose, or complain about patients, family members, caregivers, members, visitors, or community members.

Employees should not post about difficult patient encounters, unusual medical conditions, emergency situations, patient behavior, or private family interactions.

Even vague posts can create privacy risk if someone can identify the patient, facility, date, condition, or event.

- Posting about a patient's diagnosis
- Sharing a story from a shift that identifies a patient
- Recording a patient or family member without approval
- Commenting publicly on a patient complaint
- Posting photos from restricted clinical areas
- Making jokes about patients, families, or medical conditions
- Sharing screenshots from patient records or internal systems

7. Protect Confidential Company Information

Employees may not disclose confidential or non-public [Company Name] information online.

- Internal reports
- Business strategy
- Financial information
- Contracts and vendor terms

- Staffing plans
- Internal emails or messages
- Training materials
- Policies not intended for public release
- Security procedures
- Incident response information
- Legal matters
- Internal investigations
- Employee records
- Provider credentialing information
- System access details
- Non-public announcements
- If information is not public, employees should not make it public. When in doubt, do not post. Ask [Department or Role] first.

8. Do Not Speak for [Company Name] Unless Authorized

Employees may not present personal opinions as official statements from [Company Name]. Unless specifically authorized, employees should not use language that suggests they are speaking on behalf of the organization.

Employees should refer media inquiries, legal questions, regulatory questions, investor questions, public complaints, and crisis-related issues to [Department or Role].

- Avoid phrases such as: “[Company Name] believes...”, “Our official position is...”, “We are announcing...”, “On behalf of [Company Name]...”, and “The company will...”

9. Disclose Your Connection to [Company Name]

Employees should be transparent about their relationship with [Company Name] when posting about company-related matters.

If an employee discusses [Company Name], its services, care programs, facilities, products, competitors, partners, or industry issues related to their role, they should disclose that they work for [Company Name].

> **Example disclosures**
>
> *"I work for [Company Name], but these are my own views."*
> *"I am a [Company Name] employee, and this is my personal opinion."*
> *"I work in healthcare, but I am not speaking on behalf of [Company Name]."*

10. Professional Conduct Online

Employees are expected to follow [Company Name] conduct standards online just as they would at work.

Employees may not use social media to harass, threaten, bully, intimidate, discriminate against, dox, or target patients, coworkers, providers, vendors, applicants, community members, or members of the public.

- Prohibited conduct may include racist comments, sexist comments, religious harassment, disability-related harassment, age-related harassment, sexual harassment, threats of violence, bullying, posting private information about others, mocking patients or coworkers, encouraging harassment by others, and retaliation for reporting a concern.

- This policy applies even when posts are made from personal accounts or outside work hours if the conduct affects patients, coworkers, the workplace, or [Company Name].

11. Employee Rights Are Respected

Nothing in this policy is intended to prevent employees from discussing wages, hours, schedules, staffing, workplace safety, working conditions, benefits, union activity, or other rights protected by law.

Employees may have the right to discuss workplace concerns with coworkers, government agencies, labor organizations, or others.

Employees should still avoid sharing patient information, protected health information, confidential business information, private employee records, security-sensitive information, or trade secrets when discussing workplace concerns.

12. Medical Advice and Health Information

Employees should be careful when discussing medical topics online.

Employees may not provide patient-specific medical advice on social media unless it is part of an approved job responsibility and follows [Company Name] procedures.

Employees should not create confusion between general health education and a provider-patient relationship.

- Employees should not make false, misleading, unverified, or exaggerated claims about treatments, medications, medical devices, procedures, clinical outcomes, patient results, insurance coverage, care availability, safety, effectiveness, costs, or wait times.
- Employees should direct individuals seeking care or medical advice to appropriate [Company Name] channels.

13. Photos, Videos, and Recordings at Work

Employees may not take or post photos, videos, livestreams, or recordings in restricted or private areas unless authorized.

- Restricted areas may include exam rooms, patient rooms, nursing stations, operating rooms, emergency departments, pharmacies, labs, imaging areas, behavioral health areas, registration desks, billing areas, medical records areas, employee-only areas, areas showing patient information, and areas showing security systems or restricted operations.
- Employees should not record patients, visitors, coworkers, providers, or contractors without permission where required by law or company policy.
- Employees should not create social media content that interferes with patient care, safety, privacy, operations, or professional duties.

14. Official Company Accounts

Only authorized employees may manage or post from official [Company Name] social media accounts.

- Use approved login and security procedures
- Use multi-factor authentication where required
- Protect credentials

- Follow brand guidelines
- Use approved images, videos, copy, and disclaimers
- Respect copyright and trademark rules
- Protect patient and employee privacy
- Follow approval workflows
- Avoid personal opinions from official accounts
- Escalate sensitive issues quickly
- Report access issues immediately
- Never share passwords outside approved systems
- When an employee leaves [Company Name] or changes roles, account access must be removed promptly.

15. Media, Legal, Regulatory, and Crisis Situations

Employees may not post on behalf of [Company Name] about legal matters, investigations, lawsuits, patient incidents, security incidents, data incidents, public controversies, regulatory matters, workplace violence, emergency events, or crisis situations unless authorized.

Employees should not respond publicly to reporters, attorneys, regulators, influencers, activists, patients, families, or community members on behalf of [Company Name] unless it is part of their approved role.

If contacted by the media or asked to comment publicly on company matters, employees should refer the request to [Department or Role].

16. Security, Scams, and Impersonation

Employees should be alert for phishing attempts, impersonation, fake accounts, suspicious links, fake patient outreach, social engineering, and account takeovers.

- Fake [Company Name] accounts
- Impersonation of employees, providers, executives, departments, or facilities
- Suspicious messages asking for company or patient information
- Requests for passwords or login codes
- Fraudulent job postings
- Fake patient support accounts
- Account takeovers
- Security incidents involving social media
- Report concerns to [Security Contact or Department].

17. Reviews, Testimonials, and Endorsements

Employees may not post fake reviews, misleading reviews, anonymous endorsements, or undisclosed promotions of [Company Name] services.

If employees review, recommend, defend, or promote [Company Name] services, they must disclose that they work for [Company Name].

Employees may not pressure patients, families, coworkers, vendors, or community partners to post positive reviews.

Employees may not offer unauthorized rewards, discounts, gifts, benefits, or special treatment in exchange for reviews or testimonials.

Patient testimonials, success stories, and marketing content must be approved by [Department or Role] and supported by required authorization.

18. Managers and Supervisors

Managers and supervisors have additional responsibilities and should model good judgment online.

- Managers should not pressure employees to connect on personal social media accounts.
- Managers should not ask employees or applicants for social media passwords.
- Managers should not use personal social media to monitor, harass, intimidate, or retaliate against employees.
- Managers should not discuss private employee matters online.
- Managers should not post about employee discipline, performance, attendance, accommodations, complaints, investigations, or terminations.
- Managers should not encourage employees to post company content without proper disclosure.
- Managers should contact [Department or Role] when unsure how to handle a social media issue.

19. Copyright, Trademarks, and Content Ownership

Employees should not post content that belongs to someone else unless they have permission or the content is approved for use.

- Images
- Videos
- Music
- Logos
- Medical illustrations
- Training materials
- Internal documents
- Patient education materials
- Screenshots from internal systems
- Vendor content
- Partner content
- Conference materials
- AI-generated content that has not been reviewed
- Employees may not misuse [Company Name] trademarks, logos, facility names, service names, slogans, or brand assets.

20. Use of AI-Generated Content

Employees should be careful when using AI tools to create social media content related to healthcare topics or [Company Name].

Employees may not enter patient information, protected health information, confidential company information, internal documents, medical records, security details, or private employee information into unapproved AI tools.

AI-generated content for official [Company Name] accounts must follow review and approval processes.

Employees are responsible for checking AI-generated content for accuracy, privacy risks, bias, copyright concerns, and misleading health claims before posting.

21. When to Ask for Help

Employees should ask [Department or Role] before posting if content involves:

- Patient information
- Photos or videos from work
- Medical advice
- Clinical topics
- Confidential company information
- Legal matters
- Security issues
- Media requests
- Public complaints
- Reviews or testimonials
- Promotions or campaigns
- Company logos or trademarks
- Coworker concerns
- Sensitive workplace topics
- Anything that could be mistaken for an official company statement
- Questions should be directed to [Contact Email or Channel].

22. Reporting Concerns

Employees should report social media activity that may violate this policy or create risk for [Company Name].

- Patient privacy concerns
- Disclosure of protected health information
- Disclosure of confidential company information
- Harassment or threats
- Fake company accounts
- Impersonation
- Unauthorized use of logos
- Security risks
- Unauthorized media comments
- Misleading health claims
- Unauthorized patient testimonials
- Photos or videos from restricted areas
- Reports can be made to [Department or Role], [HR Contact], [Privacy Contact], [Security Contact], [Legal Contact], or [Anonymous Reporting Channel if applicable].
- [Company Name] prohibits retaliation against employees who report concerns in good faith.

23. Policy Violations

Violations of this policy may result in corrective action, up to and including termination of employment, depending on the facts, applicable law, and company policy.

- Sharing patient information
- Sharing protected health information
- Posting photos or videos from restricted areas without approval
- Sharing confidential company information

- Speaking for [Company Name] without authorization
- Harassing patients, coworkers, or others online
- Posting misleading health claims
- Misusing company logos or trademarks
- Using official accounts without approval
- Sharing account passwords
- Posting unauthorized testimonials or promotions
- Retaliating against protected activity or good-faith reporting
- [Company Name] will review each situation based on the facts, applicable law, company policy, and business impact.

24. Related Policies

Employees should also review and follow related [Company Name] policies, including:

- Code of Conduct
- Employee Handbook
- HIPAA or Patient Privacy Policy
- Information Security Policy
- Confidentiality Policy
- Acceptable Use of Technology Policy
- Anti-Harassment and Anti-Discrimination Policy
- Media Relations Policy
- Marketing and Communications Policy
- Patient Photography and Recording Policy
- Records Retention Policy
- AI Use Policy
- Incident Reporting Policy
- Disciplinary Action Policy

25. Employee Acknowledgment

I acknowledge that I have received and reviewed the [Company Name] Employee Social Media Policy. I understand that I am responsible for following this policy when using social media in ways that relate to [Company Name], patients, members, coworkers, providers, facilities, services, business partners, or reputation.

I understand that this policy does not prevent me from exercising rights protected by applicable law, including rights related to wages, hours, working conditions, protected concerted activity, reporting legal concerns, or participating in investigations.

Employee Name	
Employee Signature	
Date	
Manager or HR Representative	

Implementation checklist

Before distribution, replace bracketed placeholders, align the policy with applicable law and internal procedures, confirm reporting contacts, and obtain approval from HR, legal, privacy, compliance, security, and communications leadership.