

Social Media: Legal Issues in the Healthcare Industry

Kim C. Stanger

(8/16)



Preliminaries

This presentation is similar to any other legal education materials designed to provide general information on pertinent legal topics. The statements made as part of the presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speaker. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of law to your activities, you should seek the advice of your legal counsel.

Preliminaries

- Written materials:
 - .ppt slides
 - AMA, Guidelines on Use of Social Media
 - NCSBN, *A Nurse's Guide to the Use of Social Media*
 - Article, *Myriad of Social Media Privacy Laws Create Havoc for Multi-State Employers*
 - Article, *Drafting Employee Handbook Policies That Pass NLRB Muster*
 - NLRB, Advice Memo re Social Media
 - NLRB, “Approved” Social Media Policy
- Presentation will be recorded and available for download at www.hhhealthlawblog.com.
- If you have questions, please submit them using chat line or e-mail me at kcstanger@hollandhart.com.

Social Media: Everyone's Doing It!

- By providers / employers
 - Marketing and public relations
 - Communicate with other providers, professionals, employees and patients
 - Recruiting
 - Education
 - Research
- By employees
 - Establish professional contacts (e.g., LinkedIn)
 - Promote employer
 - Private use
- By patients
 - Communicate with providers
 - Research and share
 - Private use



Social Media: Legal Issues

- Issues to cover today:
 - Health records
 - Privacy and security
 - Responding to negative online reviews
 - Employment
 - Other liabilities
 - Suggestions for minimizing liability



Social Media: Legal Issues

- This is an overview of some of the legal issues.
 - Consult with your attorney when applying.
- We'll focus on federal laws.
- Beware additional state laws.
 - Online privacy and data breach reporting.
 - Use of social media in employment.
 - Fair business practices.
- Law is changing to catch up to technology.
 - NLRB guidance.
 - Cases.

Social Media = Medical Record?



Social Media = Medical Record?

- **“Medical record” depends on context.**
 - **Internal operations:** records you use to make treatment decisions or document interactions.
 - **HIPAA:** must produce records in “designated health set”.
 - **Subpoena, order or statutory obligation to produce:** must produce records requested regardless of how you may define “medical record”.

Social Media = Medical Record?

- Are social media communications part of the “medical record” or should they be?
 - Do they contain medical advice by one of your providers?
 - Do they contain relevant clinical or other data—
 - Intended for your providers?
 - Relevant to your provider’s treatment of the patient?
 - Relevant to relationship with patient even if the info is not clinical (e.g., disruptive conduct, complaints, etc.)
 - Do you need the communications to document events?

Social Media = Medical Record?

- Incorporation of social media content into the medical record raises practical concerns:
 - Knowledge of its existence
 - Accessibility
 - Accuracy and reliability
 - Privacy and security
 - Other?

Social Media = Medical Record?

- HIPAA grants patients rights to their “designated record set”, i.e.,
 - (1) A group of records maintained by or for a covered entity that is:
 - (i) The medical records and billing records about individuals maintained by or for a covered health care provider...; or
 - (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.
 - (2) “Record” means any item, collection, or grouping of info that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.”
(45 CFR 164.501).

Social Media = Medical Record?

- To what extent do you have obligations to produce or provide access to social media content to persons who request it in response to a subpoena, warrant, court order, or discovery request?
 - E.g., request for “all medical records relating to the patient”?
 - E.g., request includes “all records relating to the patient, whether electronic or oral”?
 - E.g., request includes “all communications to, from, or regarding the patient”?

Social Media = Medical Record?

- Consider application of existing medical record policies and procedures to social media.
 - Definitions
 - Auditing and monitoring
 - Production
 - Retention
 - Destruction
 - Privacy and security
 - Improper disclosures
 - Vulnerability to cyber attacks

Cybersecurity



Social media is a channel for cyberattack.

- **Direct messaging:** message contains malicious links.
 - E.g., recent ransomware attacks.
- **Impersonation:** attackers use false profiles to gather info, reconnoiter, or disseminate malicious links.
 - E.g., hackers used info to identify Anthem weaknesses
- **Account takeover:** attackers take over social media platform to disseminate false messages.
 - E.g., cybercriminals took over NFL Twitter account
- **Information leakage:** criminals misuse information already published.

Patient Privacy and Security



Patient Privacy

www.propublica.org/article/inappropriate-social-media-posts-by-nursing-home-workers-detailed#

Don't Miss: [The Breakdown](#) [Terror in Little Saigon](#) [Dollars for Docs](#) [Surgeon Scorecard](#) [Red Cross](#) [Workers' Comp](#)

[Donate](#)



Journalism in the Public Interest

Receive our top stories daily

Email address

[SUBSCRIBE](#)

[Home](#) [Investigations](#) [Data](#) [MuckReads](#) [Get Involved](#) [About Us](#)



Search ProPublica



Policing Patient Privacy



Inappropriate Social Media Posts by Nursing Home Workers, Detailed



Below are details of 47 incidents since 2012 in which workers at nursing homes and assisted-living centers shared photos or videos of residents on social media networks. The details come from government inspection reports, court cases and media reports.



by [Charles Ornstein](#) and [Jessica Huseman](#), ProPublica, Dec. 21, 2015, 8 a.m.

4 Comments



This is part of an ongoing investigation

[Policing Patient Privacy](#)

ProPublica is exploring how patient privacy violations are affecting patients and the medical care they receive.



[4 Stages to a Heart Attack](#)



[4 Signs](#)

The Cardiac Killer

Patient Privacy

Common privacy snafus

- Provider or employee posts patient info (“PHI”) without authorization.
 - E.g., nurse describes day at the facility.
- Provider/agent posts or sends unauthorized photo or video.
 - E.g., physical therapist sent photo of patient to therapist’s wife.
 - E.g., photo includes confidential info about others.
- Patient posts something and provider or employee responds.
 - E.g., nurse tweeted response to governor’s request.
- Provider “friends” patient or family member.
 - E.g., discussion posted on wall.
- Provider discloses more than is minimally necessary or beyond that which is authorized by patient.

Patient Privacy: Applicable Laws

- **HIPAA**
 - Privacy
 - Security(42 CFR part 164)
- **Licensing Regulations**
 - Facilities
 - Individuals
- **State Privacy Laws**
 - Medical info
 - Data breach reporting
- **Common Law Privacy Torts**
 - Appropriating plaintiff's identity for defendant's benefit.
 - Placing plaintiff in false light in public eye.
 - Publicly disclosing private facts about plaintiff.
 - Unreasonably intruding upon seclusion or solitude of the plaintiff.

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-16
Baltimore, Maryland 21244-1850



Center for Clinical Standards and Quality/Survey & Certification Group

Ref: S&C: 16-33-NH

DATE: August 5, 2016

TO: State Survey Agency Directors

FROM: Director
Survey and Certification Group

SUBJECT: Protecting Resident Privacy and Prohibiting Mental Abuse Related to Photographs and Audio/Video Recordings by Nursing Home Staff

Memorandum Summary

- **Freedom from Abuse:** Each resident has the right to be free from all types of abuse, including mental abuse. Mental abuse includes, but is not limited to, abuse that is facilitated or caused by nursing home staff taking or using photographs or recordings in any manner that would demean or humiliate a resident(s).
- **Facility and State Agency Responsibilities:** This memorandum discusses the facility and State responsibilities related to the protection of residents. Specifically, at the time of the next standard survey for both the Traditional survey and QIS, the survey team will request and review facility policies and procedures that prohibit staff from taking, keeping and/or distributing photographs and recordings that demean or humiliate a resident(s).

Background

Recent media reports have highlighted occurrences of nursing home staff taking unauthorized photographs or video recordings of nursing home residents, sometimes in compromised positions. The photographs are then posted on social media networks, or sent through multimedia messages.

HIPAA: Criminal Penalties

- Applies if employees or other individuals obtain or disclose PHI from covered entity without authorization.


Conduct	Penalty
Knowingly obtain info in violation of the law	<ul style="list-style-type: none">• \$50,000 fine• 1 year in prison
Committed under false pretenses	<ul style="list-style-type: none">• 100,000 fine• 5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	<ul style="list-style-type: none">• \$250,000 fine• 10 years in prison

(42 USC 1320d-6(a))

HIPAA: Civil Penalties

Conduct	Penalty
Did not know and should not have known of violation	<ul style="list-style-type: none">• \$100 to \$50,000 per violation• Up to \$1.5 million per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty
Violation due to reasonable cause	<ul style="list-style-type: none">• \$1000 to \$50,000 per violation• Up to \$1.5 million per type per year• No penalty if correct w/in 30 days• OCR may waive or reduce penalty
Willful neglect, but correct w/in 30 days	<ul style="list-style-type: none">• \$10,000 to \$50,000 per violation• Up to \$1.5 million per type per year• Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	<ul style="list-style-type: none">• At least \$50,000 per violation• Up to \$1.5 million per type per year• Penalty is mandatory

Text Resize **A A A**

Print 

Share   

HIPAA News Releases & Bulletins

[Advocate Health Care Settles Potential HIPAA Penalties for \\$5.55 Million](#) – August 4, 2016

[Multiple alleged HIPAA violations result in \\$2.75 million settlement with the University of Mississippi Medical Center \(UMMC\)](#) – July 21, 2016

[Widespread HIPAA vulnerabilities result in \\$2.7 million settlement with Oregon Health & Science University](#) - July 18, 2016

[Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to \\$650,000 HIPAA Settlement](#) – June 29, 2016

[HHS Guidance Regarding Patient Safety Work Product and Providers' External Obligations](#) - June 23, 2016

[Clarification of Permissible Fees for HIPAA Right of Access - Flat Rate Option Up to \\$6.50 is Not a Cap on All Fees for Copies of PHI](#) - May 23, 2016

[Unauthorized Filming for "NY Med" Results in \\$2.2 Million Settlement with New York Presbyterian Hospital](#) - April 21, 2016

[\\$750,000 settlement highlights the need for HIPAA business associate agreements](#) - April 19, 2016

[OCR Launches Phase 2 of HIPAA Audit Program](#) – March 21, 2016

[Improper disclosure of research participants' protected health information results in \\$3.9 million HIPAA settlement](#) - March 17, 2016

HHS Office for Civil Rights in Action



OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals

omic and Clinical Health Act of 2009 and the subsequent implementation of the Health Insurance Portability and Accountability Act (HIPAA) (PHI). The root causes of breaches may indicate entity-wide and industry-wide noncompliance with HIPAA's regulations, and identify any deficiencies, and better understand compliance issues in HIPAA-regulated entities more broadly. OCR's Regional Offices in all 50 states will investigate smaller breaches (involving the PHI of fewer than 500 individuals), as resources permit.

Recent breach reports include Catholic Health Care Services (<http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/agreements/triple-s-management/index.html>), St. Elizabeth's Medical Center (<http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/2012/stolen-laptops-lead-to-important-hipaa-settlements.html>), and Hospice of North Idaho (<http://www.hhs.gov/about/news/2012/08/22/hospice-of-north-idaho-hipaa-breach>).

OCR's Regional Offices, has begun an initiative to more widely investigate the root causes of breaches affecting fewer than 500 individuals. OCR will increase its efforts to identify and obtain corrective action to address entity and systemic noncompliance related to these breaches.

HIPAA: More Reasons to Comply

- State attorney general can bring lawsuit.
 - \$25,000 fine per violation + fees and costs
- Affected individuals may sue for violations.
 - No private cause of action under HIPAA.
 - But HIPAA may establish duty of care.
 - In 2014, Walgreens was hit for \$1.44 million.
- In the future, affected individuals may recover percentage of fines or penalties.
- Must sanction employees who violate HIPAA.
- HHS is conducting audits.
- Must self-report breaches of unsecured PHI.

HIPAA Privacy

- HIPAA applies to “protected health info”, i.e., *individually identifiable health info* that:
 - Is created or received by a health care provider; and
 - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care; or the past, present, or future payment for health care; and
 - That identifies the individual; or
 - With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(45 CFR 160.103)

HIPAA Privacy

- **Cannot use or disclose PHI unless use or disclosure:**
 - **Is for treatment, payment or healthcare operations;**
 - **Is to family members or others involved in care or payment for care, patient has not objected, and don't disclose more than is reasonable;**
 - **Is allowed by exceptions under 45 CFR 164.512; or**
 - **Is consistent with a valid HIPAA-compliant authorization.**
- **Cannot use or disclose more than is minimally necessary.**
- **Must implement reasonable safeguards.**

(45 CFR 500 et seq.)

**If you wouldn't say it in an elevator,
don't post it online!**



Patient Testimonial Videos

Foot Surgery Patient

Rotator Cuff Patient

Rotator Cuff Patient

Spiral Ankle Fracture Patient

Surgery for Spiral Ankle Fracture



HIPAA Privacy

- Beware your marketing department...



HIPAA Privacy

- **HIPAA compliant authorization =**
 - Not combined with any other consent or authorization.
 - Required elements:
 - Info to be disclosed.
 - Entity(ies) who may disclose info.
 - Entity(ies) to whom info may be disclosed.
 - Purpose of disclosure.
 - Expiration date or event.
 - Signature and date.
 - Required statements:
 - Individual's right to revoke authorization.
 - Generally cannot condition treatment on authorization.
 - Disclosed info may be redisclosed and not protected.

(45 CFR 164.508)

HIPAA Privacy

- Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?
- **Answer:** Yes. The Privacy Rule allows covered health care providers to communicate electronically, such as through e-mail, with their patients, provided they apply reasonable safeguards when doing so. See 45 CFR § 164.530(c). For example, certain precautions may need to be taken when using e-mail to avoid unintentional disclosures, such as checking the e-mail address for accuracy before sending, or sending an e-mail alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted e-mail ... , safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of info disclosed through the unencrypted e-mail. In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 CFR Part 164, Subpart C.

(OCR HIPAA Privacy FAQ dated 12/15/08)

HIPAA Security

- Must implement specified physical, technical, and administrative safeguards for e-protected health info, including:
 - *Transmission security*. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
 - *Encryption (Addressable)*. Implement a mechanism to encrypt electronic protected health info whenever deemed appropriate.

(45 CFR 164.312)

HIPAA Security

- Does the Security Rule allow for sending electronic PHI (e-PHI) in an e-mail or over the Internet? If so, what protections must be applied?
- **Answer:** The Security Rule does not expressly prohibit the use of e-mail for sending e-PHI. However, the [Security Rule] standards ... require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.

(OCR FAQ [undated])

- **Omnibus Rule:** must warn person if using unsecure network.

(78 FR 5634)

HIPAA Security

- How does e-mail compare to other media forms, including social media?
 - Texts
 - Facebook
 - Skype
 - LinkedIn
 - Myspace
 - Etc.?



HIPAA Security

- **Suggestions for addressing security concerns, at least until we receive contrary direction from OCR:**
 - Obtain patient's or personal rep's consent or authorization to use social media, texts, e-mail, etc.
 - Patient has right to communicate by such means.
 - Omnibus Rule: Must warn patient of risks.
 - Exercise good judgment when determining platform and content.
 - Beware platforms to which third parties have access.
 - Beware including highly sensitive information.
 - Remember the minimum necessary rule.



in Partnership with the
National Learning Consortium 

Providers & Professionals

Patients & Families ▶

Policy Researchers & Implementers ▶

▶ Benefits of EHRs

▶ How to Implement EHRs

▶ Privacy & Security

▶ EHR Incentives & Certification

▶ Success Stories & Case Studies

▶ Resource Center

What's in IT for you?

Learn about incentives for certification and find out how you can get paid for going paperless.

[Learn More >](#)



Take the First Step Toward EHR Implementation

Whether you're just starting to think about adopting an electronic health record (EHR) system or are ready to make the change from paper records to EHRs, find out how to get started.

[Take the First Step >](#)

Achieve Meaningful Use

Already have an EHR System? Learn about the meaningful use objectives that eligible professionals and hospitals must achieve to qualify for Centers for Medicare & Medicaid Services (CMS) Incentive Programs.

[Achieve Meaningful Use >](#)

Get Local Technical Help

The EHR adoption process can be overwhelming. But you don't have to do it alone. The nationwide network of Regional Extension Centers (RECs) offers local, low-cost, on-the-ground support.

[Get Local Technical Help >](#)

Privacy & Security

Your Mobile Device and Health Information Privacy and Security



Physicians, health care providers and other health care professionals are using smartphones, laptops and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help you protect and secure health information patients entrust to you when using mobile devices.



Read and Learn

- [How Can You Protect and Secure Health Information When Using a Mobile Device?](#)
- [You, Your Organization and Your Mobile Device](#)
- [Five Steps Organizations Can Take To Manage Mobile Devices Used By Health Care Providers and Professionals](#)
- [Frequently Asked Questions \(FAQs\)](#)
- [Downloadable Materials](#)



Watch and Learn

- [Worried About Using a Mobile Device for Work? Here's What To Do!](#)
- [Securing Your Mobile Device is Important!](#)
- [Dr. Anderson's Office Identifies a Risk](#)
- [A Stolen Mobile Device](#)
- [Can You Protect Patients' Health Information When Using a Public Wi-Fi Network?](#)



HIPAA Breach Notification

- If there is breach of unsecured (i.e., unencrypted) PHI, covered entity must notify:
 - Each individual whose unsecured info has been or reasonably believed to have been accessed, acquired, used, or disclosed w/in 60 days.
 - HHS.
 - If breach < 500 persons: by March 1
 - If breach > 500 persons: w/in 60 days.
 - Media if breach > 500 persons in a state.

(45 CFR 164.400 et seq.)

HIPAA Breach Notification

- Acquisition, access, use or disclosure of protected health info in violation of privacy rules is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the info has been compromised based on a risk assessment of the following factors:
 - nature and extent of PHI involved;
 - unauthorized person who used or received the PHI;
 - whether PHI was actually acquired or viewed; and
 - extent to which the risk to the PHI has been mitigated.unless an exception applies.
(45 CFR 164.402)

HIPAA: Avoiding Penalties

- You can likely avoid HIPAA penalties if you:
 - Have required policies and safeguards in place
 - Train personnel and document training.
 - Respond immediately to mitigate and correct any violation.
 - Timely report breaches if required.

*No “willful neglect” =
No penalties if correct
violation within 30
days.*

Responding to Negative Reviews



Just because the patient discloses info does not mean that you can!



Journalism in the Public Interest

Receive our top stories daily

Email address

SUBSCRIBE



Search ProPublica

Policing Patient Privacy



Stung by Yelp Reviews, Health Providers Spill Patient Secrets

The vast majority of reviews on Yelp are positive. But in trying to respond to critical ones, some doctors, dentists and chiropractors appear to be violating the federal patient privacy law known as HIPAA.

by [Charles Ornstein](#)
ProPublica, May 27, 2016, 11 a.m.

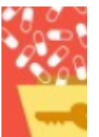
58 Comments



This is part of an ongoing investigation

Policing Patient Privacy

ProPublica is exploring how patient privacy violations are affecting patients and the medical care they receive.



4 Stages to a Heart Attack



Responding to Negative Reviews

- Do NOT disclose protected health info in online response.
 - HIPAA prohibits unauthorized use or disclosure of protected health info, including:
 - Fact that a person is or was a patient.
 - Info that could reasonably identify the patient.
 - There is no HIPAA exception for responding to a patient complaint online.
 - Patient does not waive HIPAA privacy rights by posting info online.

Responding to Negative Reviews

- Options for responding:
 - Ignore it.
 - Encourage and emphasize positive reviews.
 - Contact patient to resolve concerns or obtain consent to respond.
 - Respond generically.
 - Do not confirm or deny that complainant was a patient, or include any info about the patient or patient encounter.
 - May explain policies or practices without reference to patient.
 - Contact online company to request removal of complaint.
 - If review is defamatory, may threaten lawsuit.

Employment and Social Media



Employer's Liability

- Vicarious liability for employee's conduct within course and scope of employment.
- Negligent hiring / supervision.
- Discrimination / harassment / retaliation.
- Divulging trade secrets or proprietary information.
- Harm to reputation of employer, other employees, or third parties.
- Disclosure of information in lawsuit or otherwise.
- Privacy.

Social Media in Hiring or Evaluation

- May provide valuable info about applicant or employee.
 - Search for applicant/employee on the web.
 - Require applicant/employee to provide access to social media site as part of application process **if allowed by law.**
- Relying on info on social media may create basis for employee discrimination claim.
 - Discrimination statutes (age, race, religion, national origin, disability, sexual orientation).
 - Genetic Information Nondiscrimination Act (“GINA”).
 - Disparate impact if excludes protected classes.

Social Media in Hiring or Evaluation

Suggestions:

- Assign social media checks to someone other than decision maker; ensure the person doing the check understands limits and does not convey improper info to the decision maker.
- Check social media at end of hiring process in conjunction with background checks.
- Check only “public profile info”, not password protected info.
- Beware demanding social media passwords.
 - May violate state and perhaps federal law.
- Document appropriate factors to support decisions.

Monitoring Social Media Usage

- **Employee's use of employer's network**
 - **Electronic Privacy Communications Act (“EPCA”) and Stored Communications Act (“SCA”).**
 - **Generally protect against unauthorized access to e-communications.**
 - **Do not apply if employer provides the e-system, but may apply to web-based services.**
 - **Improper access may violate employee's privacy rights.**
 - **Make sure there is no expectation of privacy.**
 - **Employee policies should confirm there is no right of privacy.**
 - **More important for public employers.**
 - **Beware password protected sites.**

Monitoring Social Media Usage

- Employee's use of social media outside of work.
 - If info is open to public, you can generally access the info.
 - If the info is private or password protected, beware improper access or use.
 - Seek and document authorization to access **if allowed by law.**
 - Do not access under false pretenses.
 - Do not use others to access if you do not have authority.

Adverse Action Based on Social Media

RS Idaho Supreme Cour x

← → ↻ www.rawstory.com/rs/2014/06/27/idaho-supreme-court-yes-you-can-be-fired-for-saying-stupid-things-on-facebook/



***Talbot v. Desert
View Care Center,
156 Idaho 517,
328 P.3d 497
(2014)***

77
Share
37
Tweet

Idaho Supreme Court: Yes, you can be fired for saying stupid things on Facebook

By Tom Boggioni
Friday, June 27, 2014 10:46 EDT

f 103 t 37 r 0 g+ p e



An Idaho nurse saw his appeal for unemployment benefits denied after the state Supreme Court ruled that his Facebook rant threatening to “slap the ever loving bat snot” out of a patient violated his employer’s social media policy.

Joseph Talbot ,of Buhl Idaho, was fired from his job at Desert View Care Center after his employer received a tip from a nursing professor over a Facebook post the professor considered unprofessional and threatening , according to **Courthouse News Service**.

Talbot v. Desert View Care Center

- **Nursing home LPN posted following on Facebook:**
“Ever have one of those days where you’d like to slap the ever loving bat snot out of a patient who is just being a jerk because they can? Nurses shouldn’t have to take abuse from you just because you are sick. In fact, it makes me less motivated to make sure your call light gets answered every time when I know that the minute I step into the room I’ll be greeted by a deluge of insults.”
- **Nursing professor who was a Facebook friend notified employer, Desert View.**
- **Desert View fired LPN, and LPN applied for unemployment benefits.**

Talbot v. Desert View Care Center

- Supreme Court upheld denial of unemployment benefits.
 - Desert View’s Social Media Policy:
 - Employees must treat others “with respect electronically as well as in-person.”
 - “Employees will at all times avoid slanderous, vulgar, obscene, intimidating, threatening, or other ‘bullying’ behavior electronically towards [others].”
 - Record showed that:
 - LPN had signed the policy stating he had read it and agreed to be bound by it.
 - LPN admitted it was discussed in staff meetings.
- *Don’t rely too much on Talbot because of unique context.*

Adverse Action Based on Social Media

- Employers may generally take action against employee for social media conduct.
- Limits on ability to take action.
 - Off-duty conduct is protected in some states.
 - Unlawful discrimination (e.g., race, religion, age, disability, sexual orientation if applicable).
 - Whistleblower.
 - For public employers, First Amendment violations if
 - Matter of public concern, and
 - Employee not acting in official role when spoke.
 - Conduct protected by NLRA.

National Labor Relations Act (“NLRA”)

- **NLRA Section 7**
 - Protects concerted activity for employees’ mutual aid and protection.
 - Gives employees the right to discuss terms and conditions of employment.
 - * Applies to non-union and union employers*
- **Recently, NLRB has brought action against employers for:**
 - Adverse action taken against employees for social media posts, and
 - Overly broad social media policies.

NLRA: “Concerted Activity”

- “An individual employee’s conduct is concerted when he or she acts ‘with or on the authority of other employees,’ when the individual activity seeks to initiate, induce or prepare for group action, or when the employee brings ‘truly group complaints to the attention of management.’ Such activity is concerted even if it involves only a speaker and a listener, ‘for such activity is an indispensable preliminary step to employee self-organization.’
- “On the other hand, comments made ‘solely by and on behalf of the employee himself’ are not concerted.”

(NLRB in *Wal-Mart*(2011))

NLRA: “Concerted Activity”

- *Knauz BMW* (9/28/12)
 - Employee fired for inappropriate Facebook post.
 - NOT protected by NLRA
 - Derogatory comments about incident at related dealership where 13-year old drove Landrover into pond.
 - Post was unrelated to terms and conditions of employee’s employment.
 - Protected by NLRA
 - Derogatory comments about employer’s decision to serve allegedly low-budget hotdogs, cookies and snacks at BMW sales events.
 - Employees had previously discussed that serving inexpensive food to potential purchasers of luxury autos would hurt sales.

NLRA: Overly Broad Policies

- An employer's rule or policy is unlawful if it "reasonably tends to chill employees in the exercise of their Section 7 rights", e.g.,
 - (1) employees would reasonably construe the language to prohibit Section 7 activity;
 - (2) the rule was promulgated in response to union activity; or
 - (3) the rule has been applied to restrict the exercise of Section 7 rights.

(Lutheran Heritage (2004))

NLRA: Overly Broad Policies

- NLRB Acting General Counsel Memoranda concerning social media policies.
 - Social media policies may be overbroad if employees could “reasonably construe” them to prohibit employee’s right to communicate regarding wages, hours and working conditions.
 - Should expressly state that policy does not prohibit NLRA-protected activity and provide clear examples of protected conduct.
 - NLRB provided sample of approved social media policy.
(*See* Memorandum 12-59 (5/30/12))
- Not binding precedent, but...

NLRA: Overly Broad Policies

- **NLRB General Counsel's report dated 3/18/15 noted concerns about:**
 - Confidentiality
 - Employee conduct toward company and supervisors
 - Conduct toward fellow employees
 - Interactions with third parties
 - Restricting use of company logos, copyrights and trademarks
 - Restricting photos and recordings
 - Restrictions on leaving work
 - Conflict-of-interest policies

NLRA

- **Review your policies and handbooks to ensure they are consistent with NLRB’s recent decisions.**
 - Beware broad terms that employees could “reasonably construe” to prohibit NLRA-protected activity.
 - Confirm that policies and handbooks do not prohibit NLRA-protected activity.
 - Include examples.
- **Before taking action based on social media conduct, ensure your action is consistent with NLRB decisions.**

www.nlr.gov/news-outreach/fact-sheets/nlr-and-social-media

reach/fact-sheets/nlr-and-social-media



NATIONAL LABOR
RELATIONS BOARD

Find Your Regional Office | Directory | 1-866-667-NLRB | Español



Search Tools

[Home](#) [Rights We Protect](#) [What We Do](#) [Who We Are](#) [Cases & Decisions](#) [News & Outreach](#) [Reports & Guidance](#)

Home » [News & Outreach](#) » [Fact Sheets](#)

The NLRB and Social Media

The National Labor Relations Act protects the rights of employees to act together to address conditions at work, with or without a union. This protection extends to certain work-related conversations conducted on social media, such as Facebook and Twitter.

In 2010, the National Labor Relations Board, an independent federal agency that enforces the Act, began receiving charges in its regional offices related to employer social media policies and to specific instances of discipline for Facebook postings. Following investigations, the agency found reasonable cause to believe that some policies and disciplinary actions violated federal labor law, and the NLRB Office of General Counsel issued complaints against employers alleging unlawful conduct. In other cases, investigations found that the communications were not protected and so disciplinary actions did not violate the Act.

General Counsel memos

To ensure consistent enforcement actions, and in response to requests from employers for guidance in this developing area, Acting General Counsel Lafe Solomon released three memos in 2011 and 2012 detailing the results of investigations in dozens of social media cases.

The first report, issued on August 18, 2011, described 14 cases. In four cases involving employees' use of Facebook, the Office of General Counsel found that the employees were engaged in "protected concerted activity" because they were discussing terms and conditions of employment with fellow employees. In five other cases involving Facebook or Twitter posts, the activity was found to be unprotected. In one case, it was determined that a union engaged in unlawful coercive conduct when it videotaped interviews with employees at a nonunion jobsite about their immigration status

[Sign up for NLRB Updates](#)

Resources

[Download the Mobile App](#)

[The NLRB Process](#)

[E-File Documents](#)

[E-File Charge / Petition](#)

[Fact Sheets](#)

[Graphs & Data](#)

[FAQs](#)

[Site Feedback](#)

[Forms](#)

[National Labor Relations Act \(NLRA\)](#)

Ownership of Social Media

- Employee uses social media to communicate regarding employer (e.g., blog, Twitter, LinkedIn). Employee subsequently leaves. Who owns the site, content and contacts?
 - Employee?
 - Employer?
 - Social media site?

(See, e.g., PhoneDog v. Kravitz; Eagle v. Edcomm)

- ***Suggestions:***
 - *Address ownership of workplace social media accounts in policies and contracts.*
 - *Review site terms of use carefully.*

Additional Legal Risks

CAUTION

Litigation | Disclosure of confidential information and trade secrets | Defamation | Copyright violations | Unfair competition | Competitive intelligence | Negligent hiring and retention | Damage to reputation



Additional Legal Risks

- **Malpractice liability.**
 - Creation of unintended patient relationship.
 - Patients or family communicate via social media, but providers fail to consider or respond → breakdown in communication or understanding.
 - Posting inappropriate advice on social media.
 - Posting evidence that may be used against provider in litigation.
- **Practicing across state lines without a license.**
- **Providing care without establishing appropriate patient relationship.**

Additional Legal Risks

- Violation of ethical standards, e.g.,
 - Failure to meet the community standard of care.
 - Failure to safeguard the confidentiality of patient info.
 - Abandonment of a patient.
 - Failure to supervise the activities of midlevels.
 - Exceeding professional boundaries.
 - Unprofessional conduct.
 - Violation of other law.
 - Advertising the practice of medicine in any unethical or unprofessional manner.

See AMA Ethics Opinion 9.124

Additional Legal Risks

- **Defamation, libel or disparagement.**
 - Publishing false allegations resulting in damage to others.
- **Discrimination, harassment, hostile work environment.**
 - Employer → Employees
 - Employees → Employees
 - Employer → Third parties
- **Common law privacy torts.**
 - See discussion above.

Additional Legal Risks

- **Intellectual property infringement.**
 - Using third party content without permission.
 - Sharing info protected by intellectual property laws, e.g., info, documents, photos, music, etc., e.g.
 - Copyright
 - Tradenames
 - Trade secrets
 - Misappropriation, conversion
 - Beware re-posting.

Additional Legal Risks

- **Violation of consumer protection laws.**
 - False or deceptive advertising.
 - Unfair competition.
 - Disparagement of other's products.
- **Violation of FTC Guidelines “Concerning Use of Endorsements and Testimonials” by affiliated entities (16 CFR Part 255).**
 - Must disclose financial affiliation with employer if providing testimonial.
- **Violation of restrictive covenants.**
 - Non-competition.
 - Non-solicitation.

Additional Legal Risks

- **Antitrust.**
 - Conspiracy or concerted activity regarding price fixing, boycotts, dividing markets, etc.
- **Tax-exempt entity limitations on communications.**
 - Prohibitions against political activity or lobbying.
- **Securities law violations.**
- **Fair Credit Reporting Act.**
- **Gramm-Leach-Bliley Act violations.**
- **FTC Red Flag rules.**
- **Others?**

Additional Legal Risks

- Social media platform “Terms of Use”.



Minimizing Liability



Minimizing Social Media Liability

- **Consider different contexts:**
 - Provider's/agent's use of social media for personal purposes.
 - Provider's use of social media for employment purposes.
 - Provider's use of social media for business purposes.
 - Patient's or family's use of social media while at provider.
- **Decide to what extent you want to allow social media**
 - Ban social media altogether.
 - Make social media sites inaccessible.
 - Prohibit use on employer's time.
 - Prohibit use on employer's devices.

Minimizing Social Media Liability

Establish effective social media policy.

- Specify permissible scope of staff's use of social media.
- Prohibit staff from speaking for provider without authority.
 - Staff is responsible for content of their social media.
 - Opinions and statements not made on behalf of provider.
- Identify those with authority to post for provider.
- If staff assigned to post on behalf of employer, confirm ownership of content and contacts.
- Staff must disclose relationship if comment on provider's business.

Minimizing Social Media Liability

Establish effective social media policy (cont.)

- Comply with laws and policies, e.g., HIPAA, copyright, anti-discrimination, anti-harassment, etc.
- Prohibit posting anything about patients without HIPAA-compliant authorization, including comments, stories, testimonials, photos, videos, etc.
- Prohibit posting photos or video since it may include unauthorized patient information.
- Prohibit using provider's trademark or disclosing provider's confidential info without authorization.
 - Beware NLRB Guidance.

Minimizing Social Media Liability

Establish effective social media policy (cont.)

- “Be respectful and professional to our employees, business partners, competitors and patients.”
- Provider has right to monitor and inspect communications through its networks, i.e., staff has no expectation of privacy re communications through provider’s systems.
- Beware NLRB Memorandum, Guidance and decisions.
 - Do not include language that could be “reasonably construed” to prohibit NLRA-protected activity.
 - Confirm it does not prohibit NLRA-protected activity.
 - Include examples of prohibited conduct.

Minimizing Social Media Liability

Establish effective social media policy (cont.)

- Must report violations immediately.
- Penalties for violations, including termination.
- Post policy on website, in manual, etc.
- Enforce social media policy in consistent manner.
- Review and revise the policy annually, considering changes in law, use, etc.

Minimizing Social Media Liability

- Conduct and document electronic media training.
- Conduct and document HIPAA training.
- Document staff's agreement to abide by policies.
 - Confidentiality agreement
 - Social media policy
- De-identify protected health info before posting.
- Obtain HIPAA authorization before posting patient's info.
- Obtain and document patient's consent before communicating directly with patient or family through unsecure electronic media.

Minimizing Social Media Liability

- You may not be able to control patients and family members, but you can take reasonable steps to avert problems.
 - Post privacy policies applicable to patients, e.g., personal use of photos, videos, etc.
 - Include policies in registration information.
 - Respond appropriately if you become aware of patient or family member violations.

Minimizing Social Media Liability

- **Include appropriate technical safeguards on sites.**
 - Limit access to sensitive info.
 - Limit ability to comment.
- **Include appropriate rules and disclaimers on interactive site.**
 - Prohibit offensive or illegal content.
 - Site not monitored 24/7.
 - Site does not offer and should not be used for personal medical advice; users should see their own provider.
 - Not responsible for content.
 - Reserve right to remove content at anytime.

Minimizing Social Media Liability

- Monitor your sites and social media platform sites frequently, e.g., daily.
- Patients or family may post otherwise confidential info.
 - Provider not responsible for patient's posts.
- Re posts from others, you can respond, maintain, or remove it, but NEVER edit it.
 - By editing, you become co-author.
- Remove inappropriate content ASAP.
 - Digital Millennium Copyright Act requires removal of infringing material on system controlled by service provider upon receiving notice.
- Document actions.

Minimizing Social Media Liability

- For practitioners and employees:
 - Separate personal and professional social media sites.
 - Remain professional in social media interaction.
 - Deactivate walls.
 - Don't "friend" patients or family members.
 - Don't respond to patient or family comments through social media.
 - Don't provide direct patient care through social media.
 - Consider HIPAA before posting anything related to patients.

Minimizing Social Media Liability

- Before taking action against employee for social media usage:
 - Consider NLRA issues.
 - Was this concerted activity dealing with conditions of employment?
 - Was the policy overly broad?
 - Consider possibility of employee claims.
 - Discrimination
 - Retaliation
 - Public employee's First Amendment rights
 - Consult with experienced employment attorney.

Additional Resources



Additional Resources

- **AHCA/NCAL, Social Media Guidance for Nursing Care Centers and Assisted Living Communities (6/10/16), available at <https://www.propublica.org/documents/item/2991535-2016-Social-Media-Guidance.html>**
- **Sample social media policies online.**
 - **Make sure they comply with NLRB guidance.**
 - **Make sure they fit healthcare entities.**

www.hollandhart.com/healthcare

https://www.hollandhart.com/healthcare

Healthcare | Holland & Hart

Home | View | Favorites | Tools | Help

AHLA Lists Anti-Kickback Statute CMS home CMS Stark eCFR EMTALA guidelines Gmail HH Secure HIPAA (160) HIPAA Hotmail Idaho Statutes

HOLLAND & HART

people

practices

firm

locations

news & resources

blogs

careers

diversity & inclusion

community

Contact

Disclaimer

Site Map

Healthcare

Overview

Holland & Hart provides a comprehensive health law practice serving the dynamic healthcare industry. In recent years, health care has changed, extraordinary competition, and increasingly complex regulatory change, extraordinary competition, and increasingly complex regulatory attorneys and staff skillfully respond to these challenges. As a result of healthcare law, we are able to provide coordinated services to meet the business, transactional, litigation, and regulatory needs of our clients.

Our healthcare clients include hospitals, individual medical providers, medical groups, managed care organizations (MCOs), third-party administrators (TPAs), health information exchanges (HIEs), practice managers and administrators, independent practice associations (IPAs), owners of healthcare assets, imaging centers, ambulatory surgery centers, medical device and life science companies, rehabilitation centers, and extended and eldercare facilities. We have also assisted clients with the significant changes enacted by the Affordable Care Act, including advice regarding employer and health plan compliance, health insurance exchanges, accountable care organizations, and nonprofit cooperative health plans.

[+ Read More](#)

View our [blog](#) and [webinar recordings](#) that cover HIPAA, antitrust, compliance, and more!

Webinars

Articles and Forms

[- Publications](#)

[HIPAA Privacy Rule Modified to Permit Covered Entities to Make Certain Limited Disclosures to the National Instant Criminal Background System](#)

[+ Expand All](#)

Future Webinars



- *Health Law Basics* monthly webinar series
 - 9/8/16 Marketing Traps for Healthcare Providers
 - 9/15/16 Ransomware: Legal Issues
 - 9/22/16 Medical Records
 - 10/13/16 Antitrust Issues in Healthcare
 - 10/27/16 Handling Problem Patients
- *Healthcare Update* and *Health Law Blog*
 - Under “Publications” at www.hollandhart.com.
 - E-mail me at kcstanger@hollandhart.com.

Questions?

Kim C. Stanger

Holland & Hart LLP

kcstanger@hollandhart.com

(208) 383-3913

