SOCIAL MEDIA AND THE MEDICAL STAFF

Utah Association of
Medical Staff Services

Kim C. Stanger

(11/25)

Holland & Hart

Disclaimer

This presentation is designed to provide general information on pertinent legal topics. The information is provided for educational purposes only. Statements made or information included do not constitute legal or financial advice, nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author.

This information contained in this presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. Substantive changes in the law subsequent to the date of this presentation might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.

Social Media Contexts

Private Use Outside Work

Marketing and Public Relations

Staff Recruitment

Patient Interaction, Communication and Engagement

Staff Screening and Evaluation

Staff Interaction, Communication and Engagement

Professional Interactions and Credentials

Research and Share

Holland & Hart

Hospital/Entity's Liability for Social Media

- Vicarious liability for employee's/agent's conduct within course and scope of employment or agency.
- Negligent hiring / supervision.
- Discrimination / harassment / retaliation.
- Disclosure of patient info.
- Disclosing other confidential info re staff, operations, peer review, trade secrets or proprietary information.
- Harm to reputation of hospital/entity, staff, or third parties.

Overview

- Ethical standards
- Privacy and security concerns with social media
- Using social media in credentialing and contracting process
- Monitoring social media
- Adverse action based on social media
- Liability concerns
- Minimizing liability

Application of some laws may vary depending on practitioner

Employees	Independent contractors (if properly classified)	Practitioners with medical staff membership and/or clinical privileges	Government hospital

• Subject to contract terms
  • Performance standards
  • Termination
• Discrimination laws
  • Title VII
  • ADA
  • ADEA
  • Utah Anti-Discrimination Act (UAA)
• NLRA
• State practice acts
• Conscience rights
	• Subject to contract terms
	  • Performance standards
	  • Termination
	• Discrimination laws
	  • Maybe ADA
	  • Maybe Title VI
	• State practice acts
	• Conscience rights
		• Subject to bylaws (contract)
		  • Performance standards
		  • Termination
		  • Due process
		• Discrimination laws
		  • Maybe ADA
		  • Maybe Title VI
		  • Rehab Act
		• State practice acts
		• Conscience rights
			• ADA Title II
			• First Amendment
			• Due process

If have clinical privileges, must also comply with bylaws

Provider Use of Social Media

Holland & Hart

Physician's Unprofessional Conduct

- "'Unprofessional conduct' includes …

  (17) violating the American Medical Association (AMA) Code of Medical Ethics, 2017 edition, which is incorporated by reference."

(Utah R 156-67-502)

Utah physicians must comply

AMA PolicyFinder

E-2.3.2 Search

Code of Medical Ethics

2.3.2 Professionalism in the Use of Social Media

Topic: Code of Medical Ethics
Policy Subtopic: Opinions on Consent, Communication & Decision Making (2.3 Communication with Patients)
Meeting Type: Interim
Year Last Modified: 2017
Action: NA
Type: Code of Medical Ethics

AMA Code of Medical Ethics 2.3.2 Professionalism in the Use of Social Media

"Physicians … should be aware that they cannot realistically separate their personal and professional personas entirely online and should curate their social media presence accordingly. Physicians … therefore should:

(a) When publishing any content, consider that even personal social media posts have the potential to damage their professional reputation or even impugn the integrity of the profession.

(b) Respect professional standards of patient privacy and confidentiality and refrain from publishing patient information online without appropriate consent.

(c) Maintain appropriate boundaries of the patient-physician relationship in accordance with ethics guidance if they interact with their patients through social media, just as they would in any other context.

(d) Use privacy settings to safeguard personal information and content, but be aware that once on the Internet, content is likely there permanently. They should routinely monitor their social media presence to ensure that their personal and professional information and content published about them by others is accurate and appropriate.

(e) Publicly disclose any financial interests related to their social media content, including, but not limited to, paid partnerships and corporate sponsorships.

(f) When using social media platforms to disseminate medical health care information, ensure that such information is useful and accurate based on professional medical judgment."

(https://policysearch.ama-assn.org/policyfinder/detail/E-2.3.2%20?uri=%2FAMADoc%2FEthics.xml-E-2.3.2.xml; see also AMA Ethics Opinion 9.124)

Holland & Hart

Nurse Standards of Professional Accountability

- "The following standards apply equally to the LPN, RN, and APRN licenses. In demonstrating professional accountability, a licensee shall:...
  (3) demonstrate honesty and integrity in nursing practice;...
  (12) respect patients' rights, concerns, decisions, and dignity;...
  (14) maintain appropriate professional boundaries;...
  (17) protect confidential information unless obligated by law to disclose the information;(18) accept responsibility for individual nursing actions, competence, decisions, and behavior in the course of nursing practice; ...
  (20) comply with the American Nurses Association (ANA) Code of Ethics for Nurses, 2015 edition, which is incorporated by reference."
- "'Unprofessional conduct'...
  (l) failing to comply with the American Nurses Association (ANA) Code of Ethics for Nurses, in violation of Subsection R156-31b-703a(20)."

(Utah R156-31b-703a)

Holland & Hart

American Nursing Ass'n Guidance re Social Media

"[P]rinciples to help nurses get the best out of social media while safeguarding themselves, the profession, and their patients:

1. **Be aware of your audience.** Make sure that the content of your posts is appropriate for the people who will be seeing it and may share it with others.
2. **Maintain your professionalism.** Avoid posting anything that could be considered unprofessional or inappropriate, such as photos or videos of patients.
3. **Know your social media policy.** Familiarize yourself with your employer's social media policy and adhere to it across all the social media platforms that you choose to use.
4. **Secure your social media profiles.** Review and set-up the respective privacy settings for the social media platforms that you choose to use.
5. **Share credible information only.** The dissemination of credible and reliable information protects the health and well-being of the public. Engage with respectful content. Do not share content that is harmful, disparaging, racist, homophobic, or derogatory."

(https://www.nursingworld.org/social/)

Holland & Hart

Patient Privacy

Holland & Hart

Patient Privacy: Applicable Laws

- Health Insurance and Portability Act (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.

HIPAA Privacy Rule

- HIPAA applies to protected health info (PHI), 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 applies even though the info is otherwise "public".

Note:

- HIPAA applies to info generated or obtained while the covered entity is acting in its capacity as the healthcare provider to the individual or as the health plan for the individual.
- HIPAA generally does not apply to health info obtained or maintained as employer, through credentialing, etc.

HIPAA Privacy Rule

- To "de-identify" info, must remove identifiable info, e.g.,
  - Names
  - Dates
  - Telephone, fax, and e-mail
  - Social Security Number
  - Medical Record Number
  - Account numbers
  - Biometric identifiers
  - Full face photos and comparable images
  - Other unique identifying number, characteristic, or code

Presumably PHI

(45 CFR 160.103, 164.514)

HIPAA Privacy Rule

- 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;
  - For certain public safety or government functions 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 for a permissible purpose.
- Must implement reasonable safeguards to protect PHI.

(45 CFR 500 *et seq.*)

HIPAA Privacy Rule

Common privacy snafus

- Provider or employee posts patient info 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., provider discloses info in response to negative review by patient.
- 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.

HIPAA Privacy Rule

Physician takes pictures during the procedure and posts them on social media.

Photos include name, date of birth and account number.

HIPAA Civil Penalties

Conduct	Penalty
Did not know and should not have known of violation	• $141* to $71,162* per violation • Up to $2,134,831* per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Violation due to reasonable cause	• $1,424* to $71,162* per violation • Up to $2,134,831* 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	• $14,232* to $71,162* per violation • Up to $2,134,831* per type per year • Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	• $71,162 to $2,134,831* per violation • Up to $2,134,831* per type per year • Penalty is mandatory

(45 CFR 102.3, 160.404; 85 FR 2879)

https://www.hhs.gov/press-room/ocr-settles-hipaa-with-cadia-healthcare-facilities.html

LTC facilities posted patient names, photos and other PHI in “success stories” without HIPAA-compliant authorization.

OCR settled for $182,000.

“The internet and social media are important business development tools. But before disclosing PHI through social media or public-facing websites, covered entities and business associates should ensure that the HIPAA Privacy Rule permits the disclosure…. Generally, a valid, written HIPAA authorization from an individual is necessary before a covered entity or business associate can post that individual’s PHI in a website testimonial or through a social media campaign.”

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

About HHS | MAHA in Action | Programs & Services | Grants & Co

Home > Press Room > HHS’ Office for Civil Rights Settles HIPAA Investigation of Cadia Healthcare Facilities for

FOR IMMEDIATE RELEASE
September 30, 2025

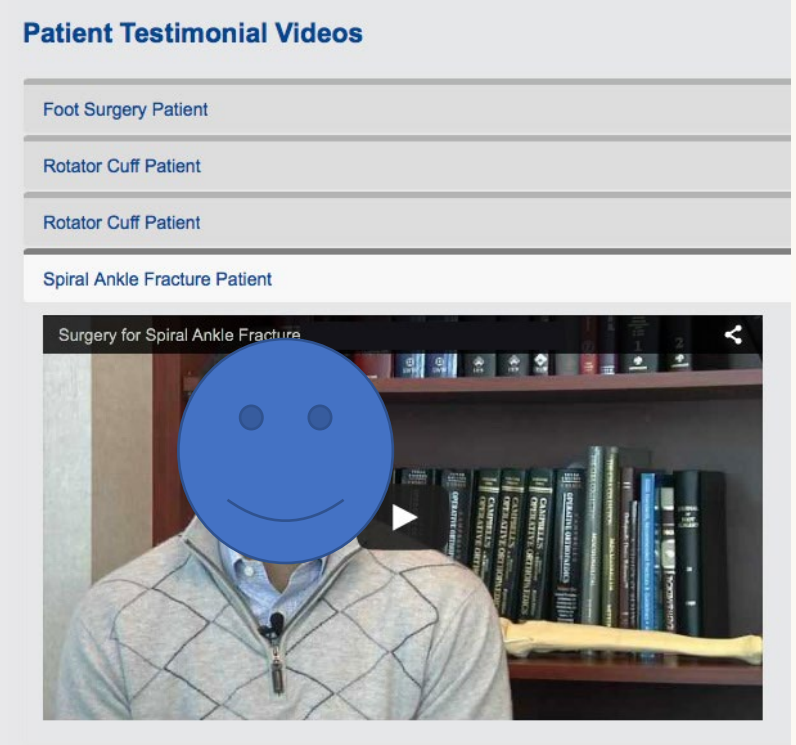
Contact: HHS Press Office
202-690-6343
Submit a Request for Comment

HHS’ Office for Civil Rights Settles HIPAA Investigation of Cadia Healthcare Facilities for Disclosure of Patients’ Protected Health Information

Settlement Resolves Potential Violations of the HIPAA Privacy and Breach Notification Rules

HIPAA Privacy Rule

- Beware your marketing department…



HIPAA Criminal Penalties

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

Conduct	Penalty
Knowingly obtain info in violation of the law	$50,000 fine 1 year in prison
Committed under false pretenses	100,000 fine 5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	$250,000 fine 10 years in prison

(42 USC 1320d-6(a))

https://www.justice.gov/usao-ndia/pr/doctor-jailed-hipaa-violations

- ER physician obtained and/or disclosed PHI of several women without authorization.
- Sentenced to 1 month in jail, $1000 fine, and 3 years supervised release.
- Likely also subject to adverse licensure action.

United States Attorney's Office
Northern District of Iowa

About News Meet the U.S. Attorney Divisions Programs Jobs

Justice.gov > U.S. Attorneys > Northern District of Iowa > Press Releases > Doctor Jailed

PRESS RELEASE

Doctor Jailed for HIPAA Violations

Thursday, January 16, 2025

Share

For Immediate Release

U.S. Attorney's Office, Northern District of Iowa

Illegally Viewed the Medical Records of Women Who Were Not His Patients at Multiple Iowa Hospitals

An Iowa emergency room doctor and medical resident, who violated the Health Insurance Portability and Accountability Act ("HIPAA") by viewing the medical records of multiple women who were not his patients, was sentenced today to a month in jail. Dr.

HIPAA Enforcement Rule

- Must self-report breaches of unsecured protected health info
  - To affected individuals.
  - To HHS.
  - To media if breach involves > 500 persons.
- In future, individuals may recover portion of penalties or settlement.
  - On 4/6/22, HHS issued notice soliciting input. (87 FR 19833)
- Must sanction employees who violate HIPAA.
- Possible lawsuits by affected individuals or others.
- State attorney general can bring lawsuit.
  - $25,000 fine per violation + fees and costs

HIPAA Privacy Rule: 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.

(45 CFR 164.508)

REQUIRED STATEMENTS

- Required statements:
- Individual's right to revoke authorization.
- Generally cannot condition treatment on authorization.
- Disclosed info may be redisclosed and not protected.

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

Responding to Negative Reviews

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

Responding to Negative Reviews

- Do NOT disclose PHI 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.

https://www.hipaajournal.com/30000-penalty-disclosing-phi-online-negative-reviews/

$30,000 Penalty for Disclosing PHI Online in Response to Negative Reviews

Posted By Steve Alder on Jun 6, 2023

The Department of Health and Human Services' Office for Civil Rights (OCR) has agreed to settle a HIPAA violation case with a New Jersey provider of adult and child psychiatric services for $30,000. In April 2020, OCR received a complaint alleging Manasa Health Center had impermissibly disclosed patient information online when responding to a negative online review. The complainant alleged Manasa Health Center's responded to a patient's review and disclosed the patient's mental health diagnosis and treatment information.

OCR launched an investigation into the Kendall Park, NJ-based healthcare provider and discovered the protected health information of a total of four patients had been impermissibly disclosed in responses to negative Google Reviews, and notified the practice about the HIPAA Privacy Rule investigation on November 18, 2020. In addition to the impermissible disclosures of PHI, which violated 45 C.F.R. § 164.502(a) of the HIPAA Privacy Rule, the practice was determined to have failed to comply with standards, implementation specifications, or other requirements of the HIPAA Privacy Rule and Breach Notification Rules – 45 C.F.R. § 164.530(i).

Manasa Health Center chose to settle the case with OCR with no admission of liability or wrongdoing. In addition to the financial penalty, Manasa Health Center has agreed to adopt a corrective action plan

"The complainant alleged [the provider] responded to a patient's review and disclosed the patient's mental health diagnosis and treatment information."

Holland & Hart

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.

HIPAA Security Rule

Holland & Hart

HIPAA Security Rule

- Must implement specified physical, technical, and administrative safeguards for e-PHI, 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)

CAUTION:

Most social media platforms do not satisfy HIPAA security rule requirements.

Non-Secure e-Communications: HIPAA Security Rule

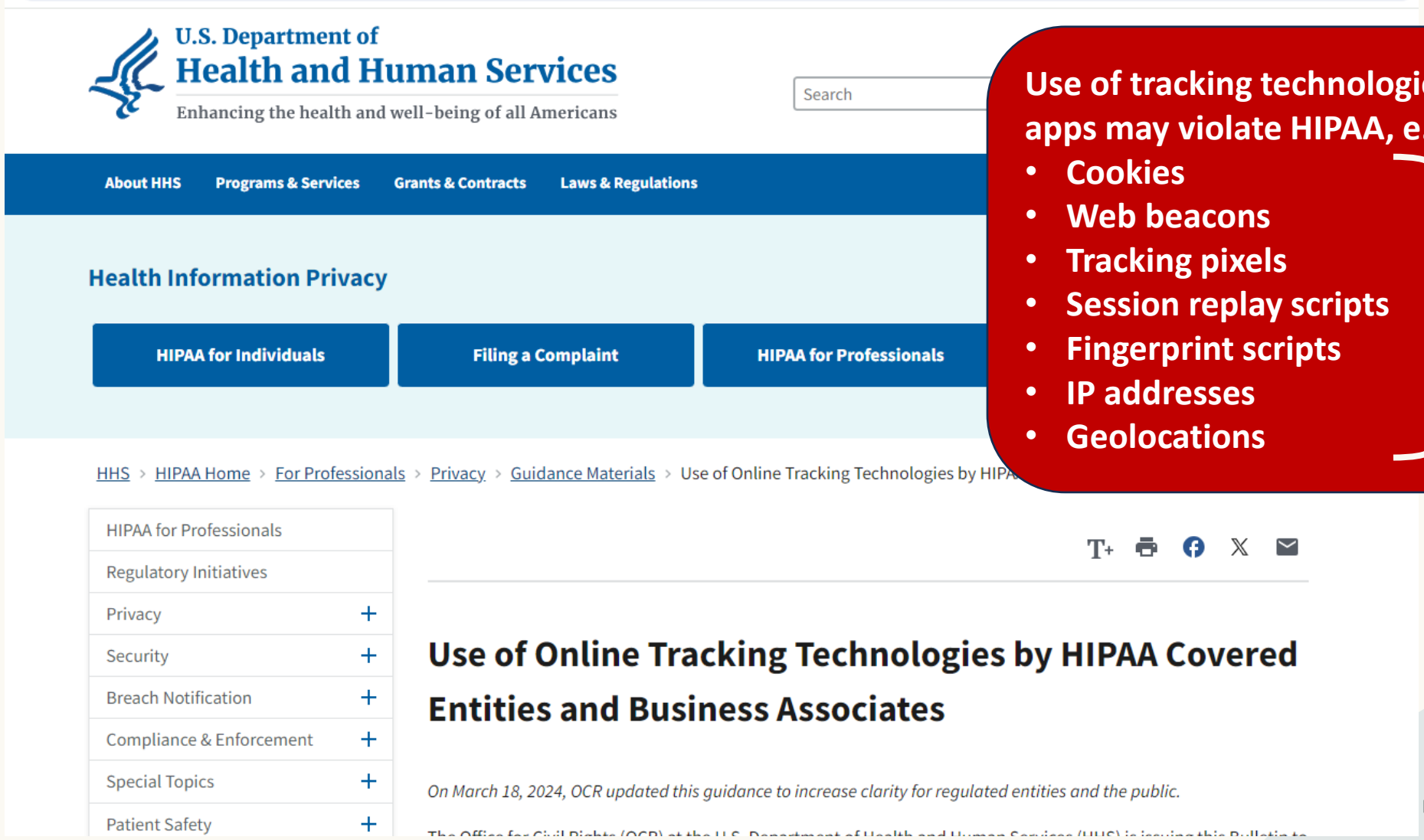
- **Does the Security Rule allow for sending electronic PHI (e-PHI) in an e-mail or over the Internet? If so, what protections must be applied?**
- **Answer:** The Security Rule does not expressly prohibit the use of e-mail for sending e-PHI. However, the [Security Rule] standards … require covered entities 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 Rule: Online Tracking



Use of tracking technologies on websites and mobile apps may violate HIPAA, e.g.,

- Cookies
- Web beacons
- Tracking pixels
- Session replay scripts
- Fingerprint scripts
- IP addresses
- Geolocations

1. Does the data contain individually identifiable info that relates to past, present, or future health, healthcare or payment?
2. If so, does HIPAA permit the use or disclosure without patient authorization?

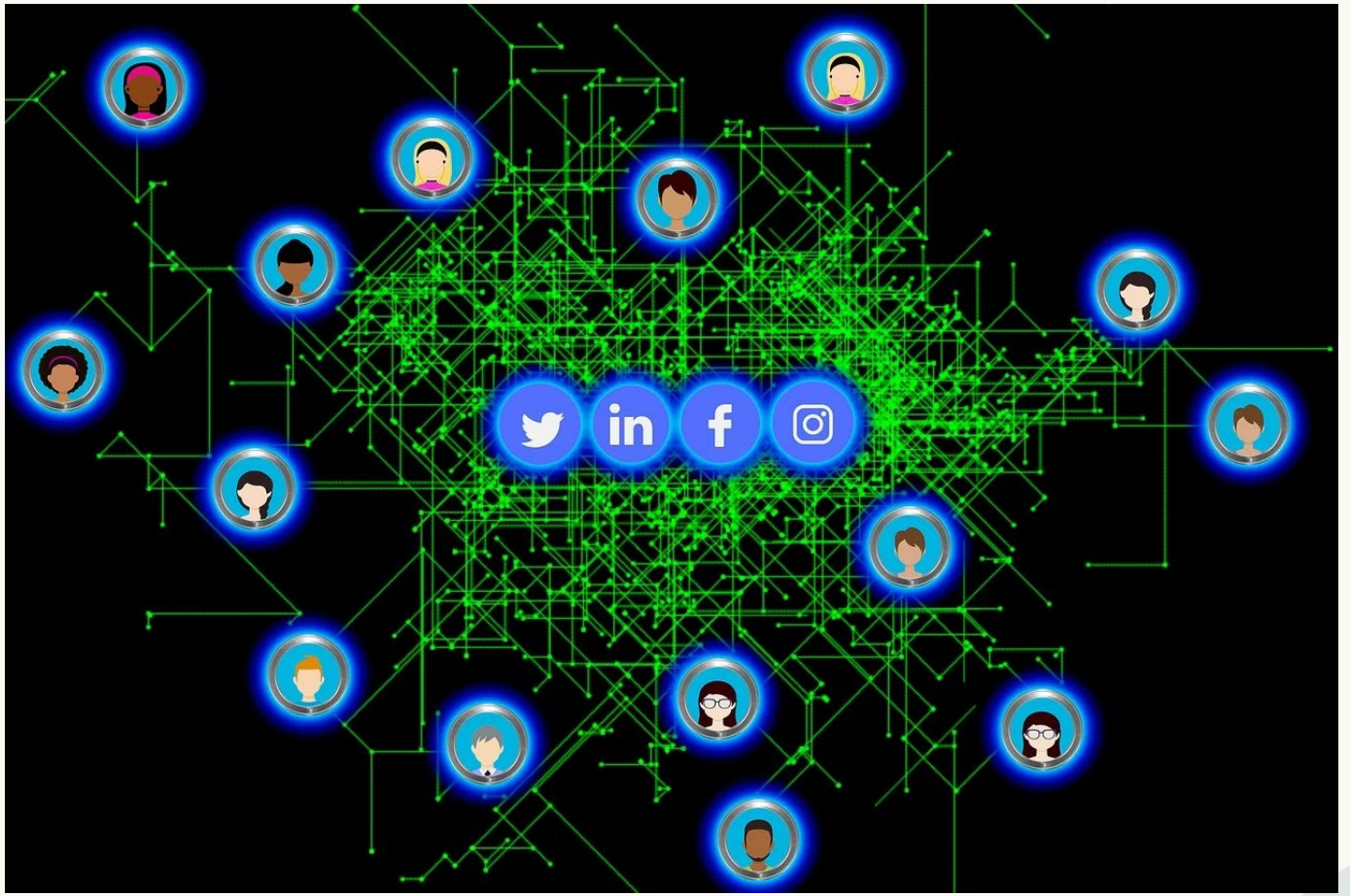
Holland & Hart

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 social media to identify and exploit 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.

Social Media in Contracting and Credentialing



Use of Social Media in Contracting and Credentialing

PROS

- Info may help assess—
  - Professional history
  - Qualifications
  - Behaviors
  - Accuracy of info provided during application or otherwise.
- Require applicant/employee to provide access to social media site as part of application process if allowed by law.

CONS

- Info may disclose info re protected status or action.
  - Race; color; sex; pregnancy; age (over 40); religion; national origin; disability; sexual orientation; gender identity; genetic info; religious, political, or personal convictions; workplace complaints; others?
- Provider may claim action was taken in violation of rights.

Utah Internet Employment Privacy Act

- **"Employer may not request disclosure of information related to personal Internet account.**

  An employer may not do any of the following:

  (1) request an employee or an applicant for employment to disclose a username and password, or a password that allows access to the employee's or applicant's personal Internet account; or

  (2) take adverse action, fail to hire, or otherwise penalize an employee or applicant for employment for failure to disclose information described in Subsection (1)."

(Utah Code 34-48-201)

- Person can sue for violations and recover up to $500

(Utah Code 34-48-301)

Utah Internet Employment Privacy Act

Employer may…

- Require employee to disclose username or password for device or account supplied or paid for by employer or used for employer's business purpose.
- Discipline or discharge employee for transferring employer's proprietary, confidential or financial info to personal internet account.
- Investigate info on personal account to ensure compliance with law or prohibitions against work-related employee misconduct.
- View, access or use info about an employee or applicant that can be obtained without the username or password or that is available in the public domain.

(Utah Code 34-48-201)

Use of Social Media in Contracting or Credentialing

EMPLOYEES

Involve knowledgeable HR Dept

Beware…

- Title VII
- ADA
- Rehab Act
- ADEA
- GINA
- NLRA
- Utah Antidiscrimination Act (UAA)
- Conscience Rights
- First Amendment (govt hospitals)
- Others?

NON-EMPLOYEES

Beware

- Maybe Title VI (public accommodations)
- ADA
  - Title II: govt entities
  - Maybe Title III (public accommodations)
- Rehab Act
- Conscience Rights
- First Amendment (govt hospitals)

Utah Antidiscrimination Act: General

- **"Discriminatory or prohibited employment practices....**

  ...

  (i) An employer may not refuse to hire, promote, discharge, demote, or terminate a person, or to retaliate against, harass, or discriminate in matters of compensation or in terms, privileges, and conditions of employment against a person otherwise qualified, because of: (A) race; (B) color; (C) sex; (D) pregnancy, childbirth, or pregnancy-related conditions; (E) age, if the individual is 40 years of age or older; (F) religion; (G) national origin; (H) disability; (I) sexual orientation; or (J) gender identity."

(Utah Code 34A-5-106)

- Plaintiff may file action with the Utah Labor Commission.

Utah Antidiscrimination Act: Expression of Belief

"Religious liberty protections – …

(2) An employee may express the employee's religious or moral beliefs and commitments in the workplace in a reasonable, non-disruptive, and non-harassing way on equal terms with similar types of expression of beliefs or commitments allowed by the employer in the workplace, unless the expression is in direct conflict with the essential business-related interests of the employer.

(3) An employer may not discharge, demote, terminate, or refuse to hire any person, or retaliate against, harass, or discriminate in matters of compensation or in terms, privileges, and conditions of employment against any person otherwise qualified, for lawful expression or expressive activity outside of the workplace regarding the person's religious, political, or personal convictions, including convictions about marriage, family, or sexuality, unless the expression or expressive activity is in direct conflict with the essential business-related interests of the employer…."

(Utah Code 34A-5-112)

Utah Conscience Law: Abortions

"**Refusal to participate, admit, or treat for abortion based on religious or moral grounds**

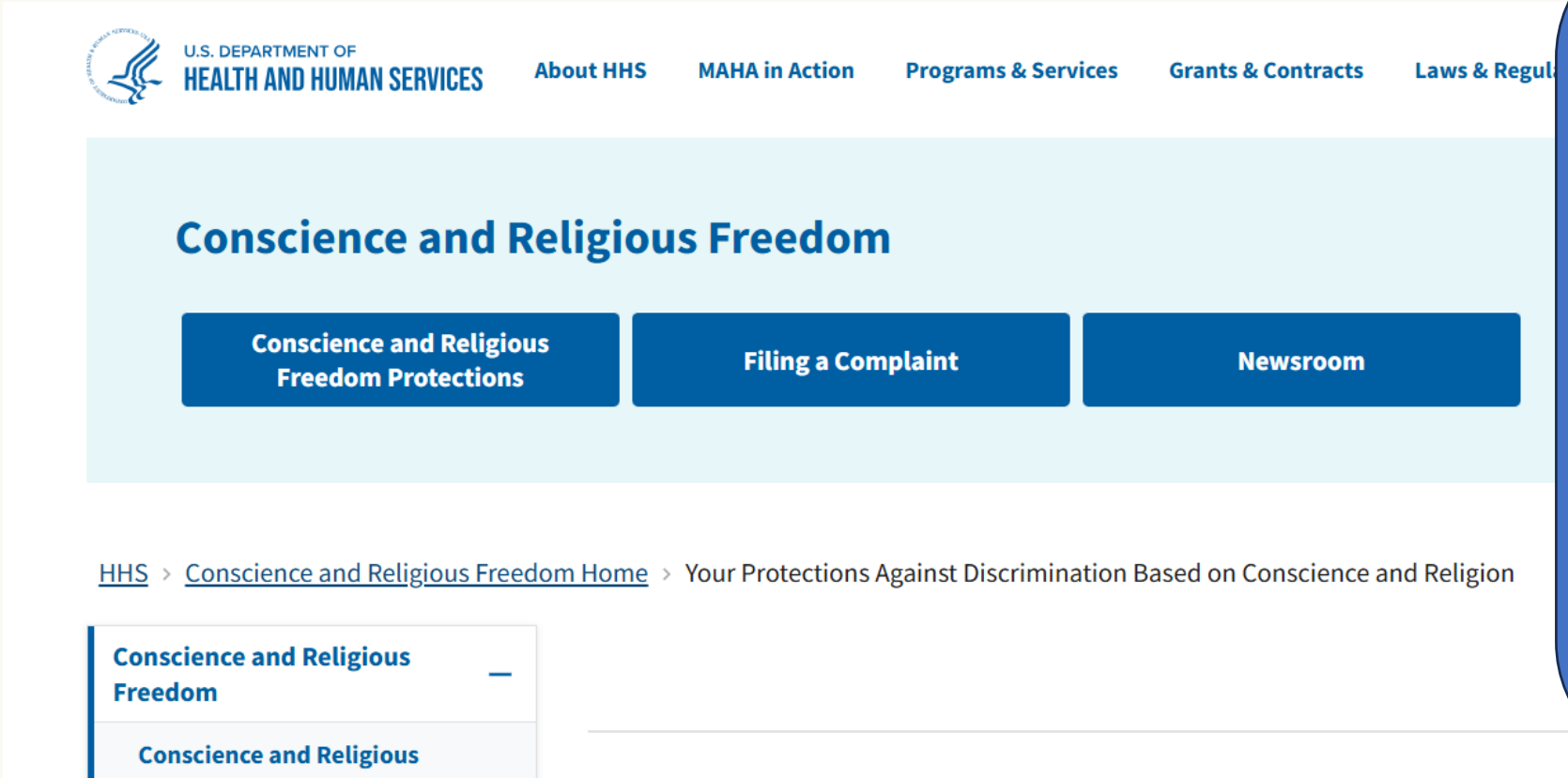
...

(5) A health care facility, employer, or other person may not take an adverse action against a health care provider for exercising the health care provider's right of refusal [to participate in an abortion], or for bringing or threatening to bring an action described in Subsection (6), including: (a) dismissal; (b) demotion; (c) suspension; (d) discipline; (e) discrimination; (f) harassment; (g) retaliation; (h) adverse change in status; (i) termination of, adverse alteration of, or refusal to renew an association or agreement; or (j) refusal to provide a benefit, privilege, raise, promotion, tenure, or increased status that the health care provider would have otherwise received.

(6) A person who is adversely impacted by conduct prohibited in Subsection (5) may bring a civil action for equitable relief, including reinstatement, and for damages. A person who brings an action under this section must commence the action within three years after the day on which the cause of action arises."

(UCA 76-7-306)

Conscience Laws



- 45 CFR part 88
- Affordable Care Act § 1553
- Church Amendments (abortion and sterilization)
- Coates-Snowe Amendment (abortion training)
- Others

Hart

Conscience Laws

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

About HHS | MAHA in Action | Programs & Services | Grants & Contracts | Laws & Regulations | Radical Transparency

Home > Press Room > HHS Investigates a Major Health System in Michigan to Safeguard Health Care Workers' Conscience Rights

Press Room

HHS Live

FOR IMMEDIATE RELEASE
June 20, 2025

Contact: HHS Press Office
202-690-6343
Submit a Request for Comment

HHS Investigates a Major Health System in Michigan to Safeguard Health Care Workers' Conscience Rights

HHS' Office for Civil Rights Reviews a Major Health System's Compliance with the Church Amendments

https://www.hhs.gov/press-room/ocr-investigates-health-system-in-michigan.html

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

United States Dept. of Labor Website

Social media activity

I was fired for chatting about my supervisor with coworkers on social media

You have the right to join with coworkers to address conditions at work. You have the right to form, join, or assist a labor organization for collective bargaining purposes or work together with coworkers to improve terms and conditions of employment. This protection extends to certain work-related conversations on social media. For example, employees have a right to address work-related issues and share information about pay, benefits, and working conditions with coworkers on social media platforms like Facebook, X, YouTube, and others.

You can't be fired, disciplined, demoted, or penalized in any way for engaging in these activities.

File a complaint with the National Labor Relations Board (NLRB)

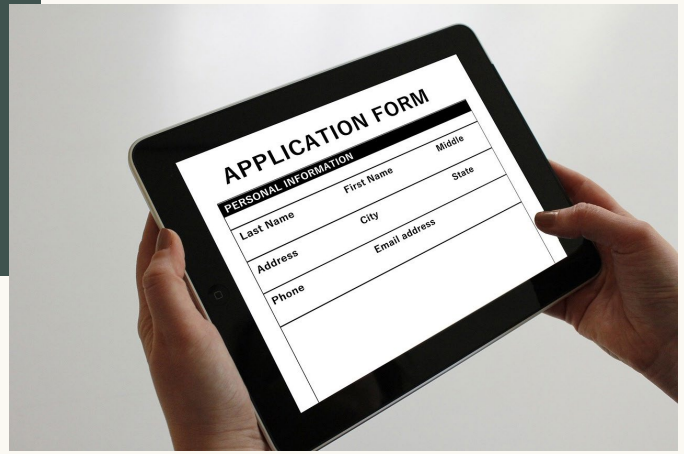
NLRA

- In the past, NLRB has taken action against employers with overly-broad social media policies.
- Review your policies and handbooks to ensure they are consistent with NRLB'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.

Public Entities: First Amendment

- Limits govt entities from taking action based on:
  - Speech
    - Social media may create a "public forum."
    - Generally, applies if:
      - Addresses matter of public concern, not purely personal grievances; and
      - Speaker not acting in official role when spoke.
    - Generally, does not apply to:
      - Personal complaints, insubordination, speech that disrupts workforce, etc.
      - Defamation, serious threat, inciting lawlessness, obscenity, etc.
    - ➢ Check with knowledgeable person before acting.
  - Religion
  - Assembly and association

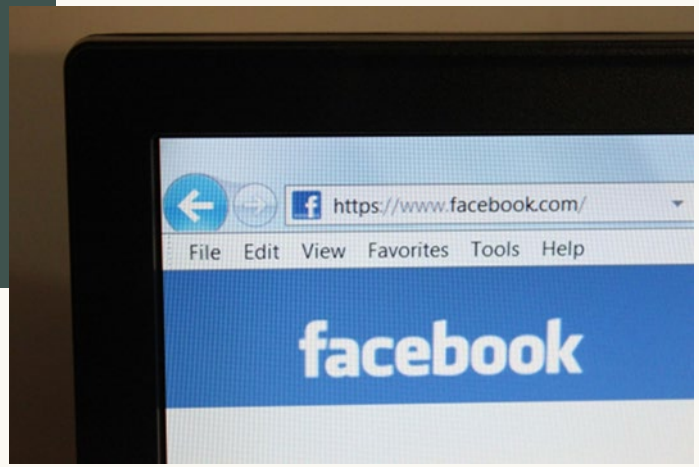
Social Media in Reviewing Application



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 or credentialing process in conjunction with background checks.
- Check only "public profile info", not password protected info.
- Beware demanding social media passwords.
- Document appropriate factors to support decisions.

Monitoring Social Media Usage: Hospital/Entity's Network

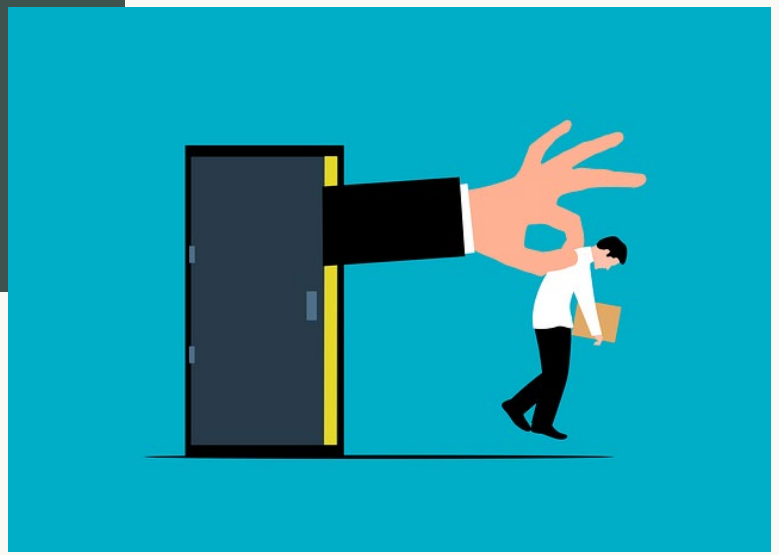


- Provider's use of hospital/entity's network
  - Utah Internet Employment Privacy Act generally allows access if employer owns device or account, but unclear effect on common law privacy rights.
  - Make sure there is no expectation of privacy.
    - Hospital/entity policies should confirm there is no right of privacy.
    - More important for public entities.
  - Beware password protected sites.
  - 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.

Monitoring Social Media Usage

- Provider's use of social media outside of hospital/entity's system.
  - 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



- Hospital/entity may generally take action against provider for improper social media conduct, but....
- Limits on ability to take action:
  - Unlawful discrimination (e.g., race, religion, age, disability, sexual orientation, etc.)
  - Off-duty expressions of religious, political, or personal convictions off-duty statements
  - NLRA
  - First Amendment
  - Conscience rights
  - Others?

Employees

Ownership of Social Media

- Provider uses social media to communicate regarding hospital/entity (e.g., blog, Twitter, LinkedIn, etc.). Provider subsequently leaves. Who owns the site, content and contacts?
  - Provider?
  - Hospital/entity?
  - Social media site?
- *Suggestions:*
  - *Address ownership of workplace social media accounts in policies and contracts.*
  - *Review site's "Terms of Use" carefully.*

Additional Legal Risks

Malpractice or Practice Violations

- 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.
  - Failure to satisfy standard of care.
  - Posting evidence that may be used against provider in litigation.
- Practicing across state lines without a license.
- Violation of telemedicine laws, e.g., providing care without establishing appropriate patient relationship.

Unprofessional Conduct

- Violation of professional or 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 APPs.
  - Exceeding professional boundaries.
  - Violation of other law.
  - Advertising the practice of medicine in any unethical or unprofessional manner.

(*See* AMA Ethics Opinion 9.124)

Common Law Torts

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

Intellectual Property

- 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.

Consumer Protection Laws

- Violation of consumer protection laws.
  - False or deceptive advertising.
  - Unfair competition.
  - Disparagement of other's products.
- FTC Guides Concerning Use of Endorsements and Testimonials in Advertising
  - Truthful
  - Disclose material connection between endorser and company

  (16 CFR 255)
- FTC Rules for Consumer Reviews and Testimonials
  - Prohibits fake, incentivized reviews.
  - Disclose reviews by employees, officers, or their immediate family members

  (16 CFR 465)

FTC Rules

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement | Policy | Advice and Guidance | News and Events | About the FTC

Endorsements, Influencers, and Reviews

Home / Business Guidance / Advertising and Marketing

https://www.ftc.gov/business-guidance/advertising-marketing/endorsements-influencers-reviews

- Advertising and Marketing
- Advertising and Marketing Basics
- Children
- **Endorsements, Influencers, and Reviews**
- Environmental Marketing

Featured

Tax-Exempt Entities

- Tax-exempt entity limitations on communications.
  - Cannot endorse, oppose, or contribute to political candidates for public office.
  - Lobbying must be insubstantial, issue-focused and/or educational.
- Others?

Minimizing Liability

Minimizing Social Media Liability

- Consider different contexts:
  - Provider's use of social media for personal purposes.
  - Provider's use of social media for entity's purposes.
  - Patient's or family's use of social media while at provider.
- Decide to what extent you want to allow social media at hospital/entity.
  - Ban social media altogether.
  - Make social media sites inaccessible.
  - Prohibit use on employer's time.
  - Prohibit photos, videos or recording on hospital/entity property.
  - Prohibit use on hospital's/entity's system or devices.
  - Limit those who can use social media on behalf of hospital/entity.

Minimizing Social Media Liability

Establish effective social media policy.

- Specify permissible scope of staff's use of social media.
- Prohibit staff from speaking for hospital/entity without authority.
  - Staff is responsible for content of their social media.
  - Opinions and statements not made on behalf of hospital/entity.
- Identify those with authority to post for hospital/entity.
- If staff assigned to post on behalf of hospital/entity, confirm ownership of content and contacts.
- Staff must disclose relationship if comment on hospital/entity'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 because it may include unauthorized patient information.
- Prohibit using provider's trademark or disclosing provider's confidential info without authorization (subject to NLRB concerns).

Minimizing Social Media Liability

Establish effective social media policy (cont.)

- "Be respectful and professional to our employees, business partners, competitors and patients."
- Hospital/entity has right to monitor and inspect communications through its networks, i.e., staff has no expectation of privacy re communications through hospital/entity's systems.
- Beware NLRA concerns.
  - Do not include language that could be "reasonably construed" to prohibit NLRA-protected activity.
  - Confirm policy 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 contract termination, adverse employment or credentialing action, etc.
- Post policy on website, medical staff rules, staff manuals, 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, e.g., in contracts, medical staff applications, bylaws, confidentiality agreements, social media policy
- De-identify PHI before posting.
- Obtain HIPAA authorization before posting PHI.
- Obtain and document patient's consent before communicating directly with patient or family through unsecure electronic media.

Minimizing Social Media Liability

But what about what patients or their families do?

- You may not be able to control patients and family members who post about your hospital/entity online, 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.
- You're not liable for what third parties do so long as you act reasonably.

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 providers and employees:
  - Separate personal and professional social media sites.
  - Remain professional in social media interaction.
  - Deactivate walls that allow posts.
  - 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.
- See ethical rules and guidelines.

Minimizing Social Media Liability

- Before taking action against employee or providers for social media use:
  - Consider state and federal laws.
  - Consider NLRA issues.
    - Was this concerted activity dealing with conditions of employment?
    - Was the policy overly broad?
  - Consider possibility of employee or provider claims.
    - Discrimination
    - Retaliation
    - Public employee's First Amendment rights
  - Consult with qualified HR personnel, attorney, etc.

Questions?

Kim C. Stanger

Holland & Hart LLP

kcstanger@hollandhart.com

(208) 383-3913

Holland & Hart