Social Media & HIPAA Privacy Challenges, Complications & Opportunities

Christie A. Moon, Esq., CHC
Principal, Moon Compliance Consulting
HCCA Alaska Regional
February 23, 2023

Your Presenter: Christie A. Moon, Esq., CHC

A health law attorney, former prosecutor, and former compliance and privacy officer, Christie has served in compliance and privacy roles for Hospitals, Physician Groups, and Health Plans. Christie has over 29 years of compliance, privacy and investigative experience.

Christie also served as Senior Counsel, Investigations for Sutter Health in Sacramento, California. Prior to joining Sutter Health, she served as National Director of Fraud Control and Special Investigations for Kaiser Permanente. Christie is also a frequent invited speaker at HCCA regional compliance events and has been a speaker at HCCA's Annual Compliance Institute several times.

In 2021, Christie retired from Sutter Health and full-time practice. She now divides her time between Seattle and Portugal and her passions include hiking the Camino de Santiago in France, Portugal and Spain and fishing in the Pacific Northwest.

In 2022, Christie formed the firm, Moon Compliance Consulting, LLC.

Christie's Live and Remote Compliance and Privacy Services Include:

- **Compliance, Privacy and Investigations Education with Interactive Case Studies**
- **Confidential and Privileged internal investigations, in partnership with you**

AGENDA – HIPAA, Social Media & Health Care

HIPAA Overview

Social Media: Challenges, Complications & Crossover issues

- Emory Healthcare Tik Tok
- University of Utah Nurse Arrest for defending privacy and HIPPA issues with Law Enforcement

Case Studies

- Reality TV Nurse fired for ER Room Post
- Provider responds to Yelp and other Social Media Scenarios

Opportunity: Patient Privacy vs. Personal Expression

- Do's and Don'ts for Health Care Workers

Opportunity: Partnering with your Media Relations Team

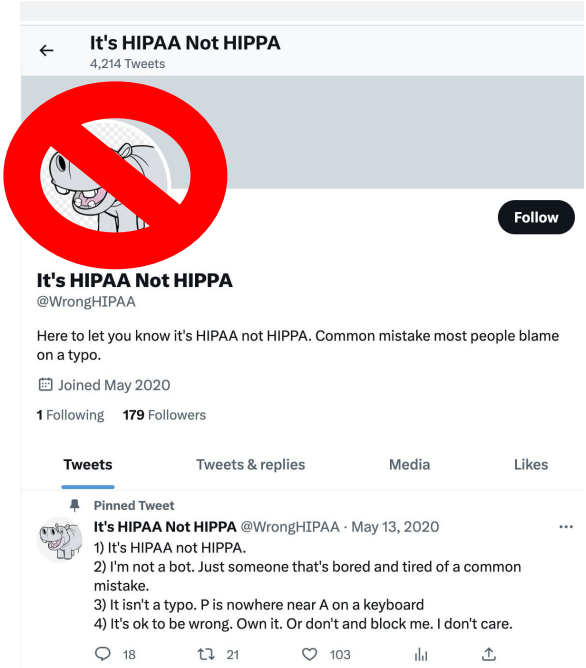
Opportunity: Do's and Don'ts for Effective Privacy Investigations into Social Media Issues

Opportunity: Sample Social Media Policy for HIPAA Regulated Entities That Provide Patient Care

Alaska State Privacy Laws: Brief Overview

Exercise: Is it a HIPAA or a Privacy Violation?

It's HIPAA not HIPPA



The HIPAA Privacy Rule

The 18 Personal Identifiers that must be removed before a record set is considered deidentified (HIPAA PHI Identifiers)

• Names or part of names	• Any other unique identifying characteristic
• Address/Geographic identifiers	• Dates directly related to a person
• Phone number details	• Fax number details
• Details of email addresses	• Social Security details
• Medical record numbers	• Health insurance beneficiary numbers
• Account details	• Certificate or license numbers
• Vehicle license plate details	• Device identifiers and serial numbers
• Website URLs	• IP address details
• Fingerprints, retinal and voice prints	• Complete face or any comparable identifying photographic images

Overview: Rules Baked into HIPAA

Privacy Rule
-Dictates how PHI can be used and disclosed
-Gives patients right to access their PHI

Security Rule
-Sets standards for protecting electronic PHI
-There are several parts

Breach Notification Rule
Requires Notification
-to Individuals Impacted
-to HHS OCR

Omnibus Rule
-Merges HITECH rules into HIPAA

Enforcement Rule
-Sets forth fine amounts
-Gov't investigation protocols

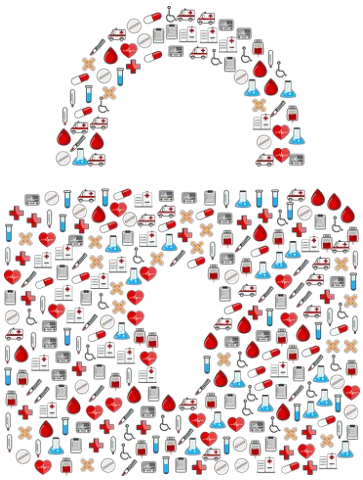
The HIPAA Privacy Rule

The Privacy Rule protects PHI from unauthorized use or disclosure, while letting providers exchange information to coordinate care.

It also gives patients the right to examine and get a copy of their medical records, including an electronic copy, and to request corrections.

Patient's can also restrict their health plan/insurance access to information about treatment they've paid for in cash.

The Privacy Rule also allows for mandatory reporting of certain types of abuse or neglect, and crimes.

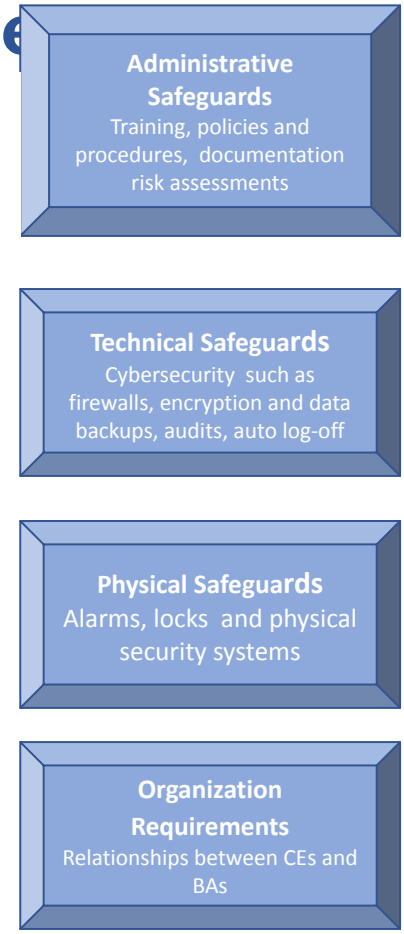


The HIPAA Security Rule

The HIPAA Security Rule establishes national standards to protect electronic PHI (ePHI) which is created, received, used or maintained by the covered entity. It includes requirements to protect the, confidentiality, integrity and availability of ePHI.

There are several parts to the Security Rule – **45 CFR Part 160, and Subparts A and C of Part 164**

The Security Rule also requires the development of appropriate security policies. Additionally, security risks must be analyzed and documented, and solutions must be created to address problems detected.



Breach Notification Rule

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification after a breach of unsecured PHI.

When a PHI breach occurs, the HIPAA Breach Notification Rule requires notification of affected individuals, HHS, and, in some cases, the media. Generally, a breach is an unpermitted use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. The unpermitted use or disclosure of PHI is a breach *unless there is a low probability the PHI has been compromised.*

Low probability is determined based on a risk assessment of:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PHI or received the disclosed PHI
- Whether an individual acquired or viewed the PHI
- The extent to which the organization was able to reduce or mitigate the PHI risk

Covered Entities must notify authorities of large breaches without reasonable delay and no later than 60 days after discovering the breach. For smaller breaches within 60 days of occurrence or at the end of the year.

The Breach Notification Rule also requires business associates to notify a covered entity of breaches at or by the business associate.

See:
https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.ht

Omnibus Rule

Omnibus Rule: The Omnibus Rule implemented most HIPAA-related changes that were part of the HITECH Act. This rule became effective March 26, 2013.

Changes to HIPAA included items in the areas of:

- PHI used in marketing or fundraising
- Selling PHI without express consent of the patient
- Student immunization disclosures
- The extension of HIPAA coverage to Business Associates (BAs) , and the Requirement for Business Associate Agreements and new penalty tiers for violations of HIPAA.

The HIPAA Enforcement Rule & OCR Fines

45 CFR Part 160, subparts C, D and E.
Should a HIPAA breach occur, the Enforcement Rule lays out how any resulting government investigations are carried out. The rule also contains provisions relating to compliance and investigations as well as penalties. Once OCR determines the CE's level of negligence, fines may be issued.

However, a fairly recent decision by the Fifth Circuit is calling OCR fines into question. In January of 2021, the Fifth Circuit vacated a $4.3 million penalty that HHS OCR had issued against the University of Texas MD Anderson Cancer Center in 2017. OCR initially levied this fine after the hospital disclosed three separate security incidents where unencrypted devices containing ePHI were stolen or lost in 2012 and 2013.

The court's decision focused on whether a "disclosure" should include a passive loss or theft of information. The appeals court found it unreasonable to consider a device theft or loss to be a "disclosure" by MD Anderson. The court also focused on the fact that this fine was much higher than those issued in similar matters. The court implied that this fine amount reflected an "irrational distinction between like cases."

Mitigating Factors for OCR Fines

1. Effectiveness and Quality of Policies
2. Effectiveness of Incident Response
3. History of Prior Issues

Common HIPAA Violations – OCR Actions

- Hackers
- Insufficient IT Security
- Fraud/ID theft by Employee
- Accidental disclosure by Employee
- Unauthorized Access
  - Snooping
  - Fraud/Medical ID theft
  - false charting

HIPAA violation

- **Stolen or Lost Devices w/failure to encrypt or otherwise secure**
- **Improper Disposal**
- **Not providing or providing untimely patient access to their records**
- **Business Associate Disclosures**
- **Failure to Notify or Untimely notification of a Breach**
- **Inadequate Access Controls**
- **Failure to perform, document and act on Risk Analysis**

TikTok

Emory University Hospital Midtown L&D Nurses

Examples of Nurse's "Icks" stated on TikTok:

- **Dad's demanding paternity tests outside the delivery room door.**
- **Delivery patient declining an epidural but reporting pain scale at 8/10 while not yet dilated.**
- **"My ick is when you ask me how much the baby weighs and its still in your hands."**
- **Complaints about patient family members asking for assistance but not using the call light (with another nurse mockingly asking for water.)**
- **Dad going room to room between two baby mamas.**

Emory Healthcare Response

A STATEMENT TO OUR COMMUNITY

EMORY HEALTHCARE IS COMMITTED TO PROVIDING EMPATHETIC, HIGH-QUALITY CARE TO OUR COMMUNITY, AND OUR PATIENTS COME FIRST.

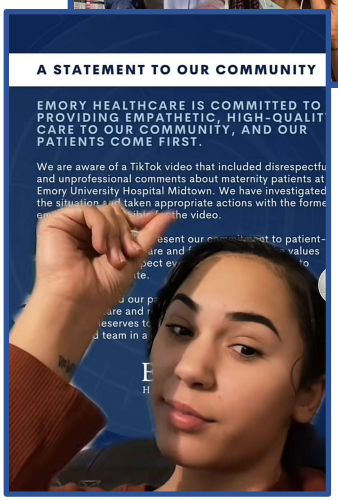
We are aware of a TikTok video that included disrespectful and unprofessional comments about maternity patients at Emory University Hospital Midtown. We have investigated the situation and taken appropriate actions with the former employees responsible for the video.

This video does not represent our commitment to patient- and family-centered care and falls far short of the values and standards we expect every member of our team to hold and demonstrate.

At no time should our patients ever feel they are not being treated with care and respect. Every patient at Emory Healthcare deserves to be cared for by a compassionate, experienced team in a comfortable and safe environment.

EMORY HEALTHCARE

Patient and Community Reactions



Negative Responses:

- 'My ick is unprofessional nurses." (67.7k likes)
- "My ick is those nurses not realizing how many of us moms have lost a child, and they feel they can judge."
- "My ick is nurses that judge you at your most vulnerable moment in time and judge your family for just trying to support you through birth."

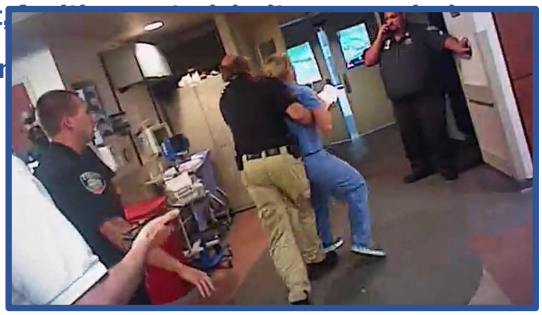
Other Responses:

Others felt the nurses should have more education on social media, or that Emory should have sent the nurses to therapy or even done more to model the compassion they were seeking from the nurses.

Social Media in the Healthcare Workplace

When does the Privacy Rule allow Covered Entities to Disclose Requested PHI to Law Enforcement?

1. **To comply with a court order, warrant, subpoena or summons issued by a judicial officer or grand jury**
2. **To respond to an administrative request in the form of a relevant and material civil administrative subpoena or summons (limited)**
3. **To respond to a request for PHI to identify to locate a suspect person (li**



Utah Nurse Arrested For Doing Her Job Reaches $500,000 Settlement

November 1, 2017 · 12:10 PM ET

LAUREL WAMSLEY

Alex Wubbels, the nurse who was arrested for refusing to let a police officer draw blood from an unconscious patient, has settled with Salt Lake City and the University of Utah for $500,000. Wubbels is shown here during an interview in September.

Rick Bowmer/AP

When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement (LE) officials?

Link:

HHS Guidance on Disclosures to Law Enforcement

- As noted on prior page when law enforcement is asking

Otherwise:

- Crime against a CE's workforce member or on the CE's premises
- To ID or apprehend a person who admitted to participation in a violent crime (except during therapy.)
- To respond to a request for PHI about the victim of a crime and the victim agrees, or if the victim is unconscious under certain circumstances
- To comply with mandatory abuse reporting requirements such as child or elder abuse
- To comply with state law reporting requirements such as gunshot or stab wounds
- To report the death of an individual

Link to FBI's guidance:

FBI HIPAA Guidance

HIPAA and Social Media

While HIPAA became law long before social media existed, with subsequent regulatory updates, it clearly impacts what can be shared online.

PHI must be kept off social media, unless express permission has been granted by the patient in writing.

This includes anything that could lead back to the patient. Violations could result in civil penalties and even action against provider licenses.

Man vs. 6 Train…#lifesaving #EMS #NYC #ER

This pic and these comments may contain at least two of the 18 HIPAA identifiers:

Geographic subdivisions smaller than a state, and their equivalent geocodes

All elements of dates directly related to an individual including …admission date

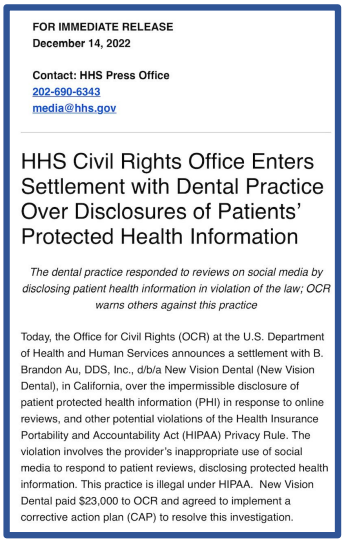
HIPAA and Responding to Patient Complaints on Social Media

Another key Social Media HIPAA risk area involves responding to social media reviews by patients.

Patients are increasingly using the internet to research providers and comment on their negative experiences. And they are well within their rights to do so.

BUT, if an organization or provider responds, they cannot in any way indicate that the patient even visited the facility or was treated. If it does, that's a HIPAA violation and OCR has recently been very aggressive in this area.

Here is a recent example of a dental practice hit with a HIPAA fine for responding to yelp reviews.



FOR IMMEDIATE RELEASE
December 14, 2022

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Civil Rights Office Enters Settlement with Dental Practice Over Disclosures of Patients' Protected Health Information

The dental practice responded to reviews on social media by disclosing patient health information in violation of the law; OCR warns others against this practice

Today, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services announces a settlement with B. Brandon Au, DDS, Inc., d/b/a New Vision Dental (New Vision Dental), in California, over the impermissible disclosure of patient protected health information (PHI) in response to online reviews, and other potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. The violation involves the provider's inappropriate use of social media to respond to patient reviews, disclosing protected health information. This practice is illegal under HIPAA. New Vision Dental paid $23,000 to OCR and agreed to implement a corrective action plan (CAP) to resolve this investigation.

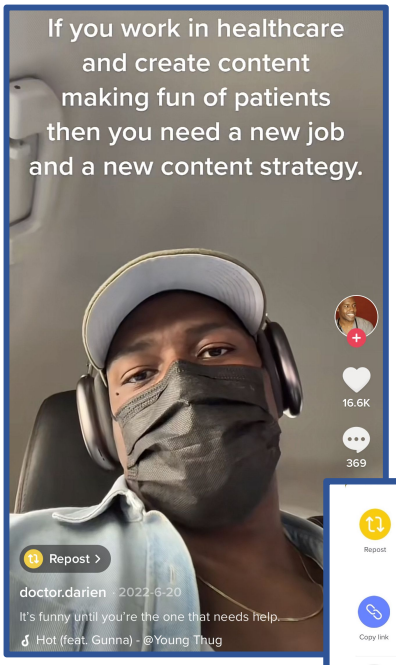
Social Media in the Healthcare Workplace

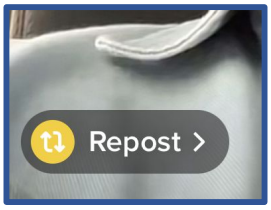
Making fun of patients on TikTok

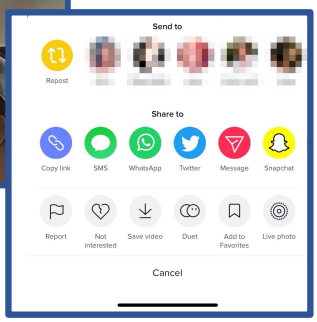
A search of TikTok for Nursing and Icks reveals quite a few examples of people making fun of patients.

While this may not be a HIPAA violation, it is often insulting to patients and harms the reputation of the person posting as well as the facility.

It's just never a good idea.







Repost and Retweet

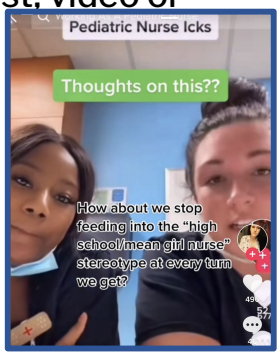
Additionally, if it is a borderline HIPAA violation or otherwise inappropriate, having the subject remove the post may not be sufficient to eliminate it. This should impact a HIPAA risk analysis.

TikTok has a "Repost" button, similar to Twitter's retweet button which typically means having the original poster delete the post, doesn't mitigate the privacy risk.

Social Media Do's and Don'ts for Healthcare Workers

DO:

- Do talk about yourself, the nursing profession, your family, hobbies and interests
- Do shed a positive light on the profession profession in posts
- Do be keenly aware of and follow your employer's social media policies
- Do realize that nothing online is ever anonymous… and that once posted, reposts and screenshots can eliminate ability to remove the post, video or other concerning social

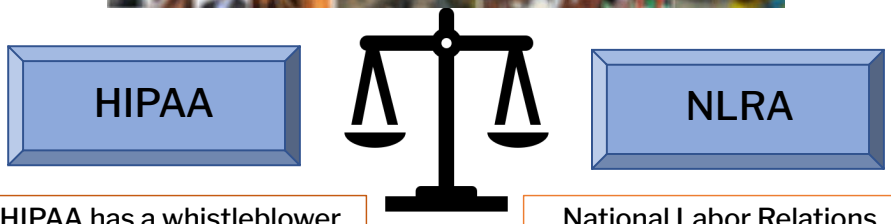


DO NOT:

- Don't ever talk about patients or coworkers
- Don't post from or near the healthcare workplace
- Don't identify your employer on social media
- Don't post anything online that you wouldn't say to your CEO, CNO or HR
- Don't do anything to degrade patients or embarrass your profession, even if it's a trend, like the ick trend

Opportunity: Effective Education on Balancing Protected Speech with HIPAA

Social Media Complaints Involving Working Conditions or Patient Safety



HIPAA has a whistleblower exception, but it doesn't include complaining on social media (45 CFR §164.502)

National Labor Relations Act (NLRA) Protects speech regarding working conditions and patient safety

Opportunity: Partnering with Media Relations

Balancing brand promotion, philanthropy strategies, and social media with compliance and privacy issues and media events.

Brand Strategy Media Support

Often Media Relations (or Public Affairs) use Social Media and Patient Stories for Brand Promotion and Philanthropy efforts
They may also assist with media engagement in sensitive matters with media inquiries

Compliance and Privacy Issues

Compliance and Privacy partnerships with Media Relations are important where you:

1) Want to collaborate on a case that has/will get media attention
2) Need to ensure that they are in compliance with HIPAA and other Privacy rules

Investigating Social Media Concerns

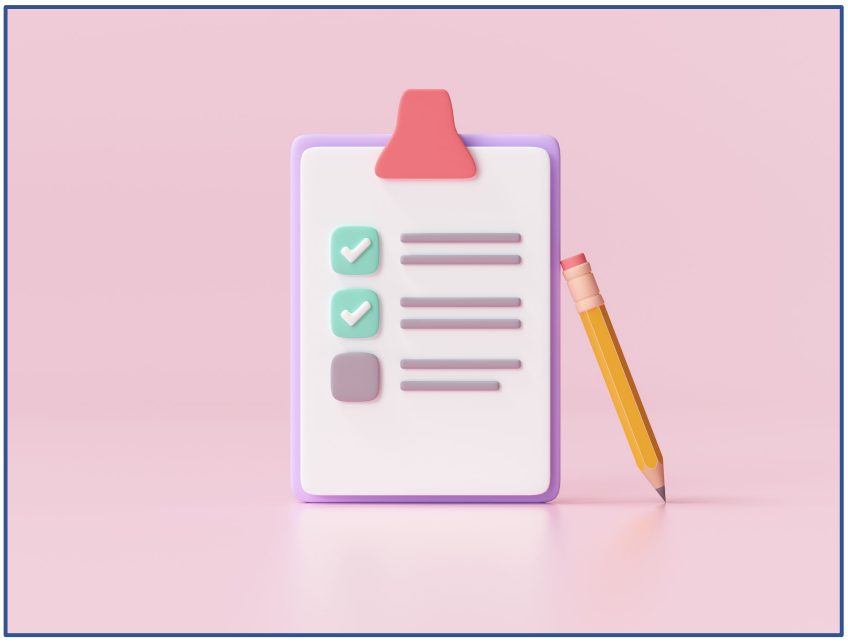
DO:

1. Do get a copy of the offending post before you interview a subject who posted something of concern
   - Get a forensic copy for high-risk cases
   - At the very least, print or scan a copy with dates where possible
   - If you don't, the original post is likely to disappear as soon as the subject finds out you're investigating.
2. Do be keenly aware of and apply your employer's social media policies and code of conduct
3. Do document facts gathered and concerns raised for analysis and decision-making
4. From a privacy risk analysis perspective, do realize that nothing online is ever anonymous… and that once posted, reposts and screenshots can eliminate ability to remove the post, video or other concerning social media
5. Do realize these must be examined from each legal/risk perspective
   - Privacy: Was HIPAA violated?
   - Employment law/NLRA: Has protected speech occurred?
   - Risk: Are there Patient Safety/Liability issues that need assessed and is corrective action needed?

DO NOT:

1. Do not ignore complaints just because complainant appears biased
2. Do not assume that having the subject take the post down solves or sufficiently mitigates privacy concerns
3. Do not take the subject's word for it that a post or picture has been taken down. Search for reposts and retweets etc., relevant to your analysis.
4. Do not forget to work with legal counsel and other stakeholders on complex analyses
5. Do not ignore other perspectives when analyzing social media activity:
   - See #5 on the "DO" column
6. Do not think that just because a post makes your facility look bad that it's a violation. Analysis m

Opportunity: Social Media Policy Sample for Covered Entities that Provide Patient Care



DISCLAIMER:
This is only a sample. It is not legal advice. It is important to review and customize your social media policy to meet your specific needs and challenges and to include other stakeholders such as HR, Employment Law, and Media Relations or Public Relations in the development of this policy.

Alaska: State Privacy Laws and HIPAA.

Although HIPAA is really the big challenge regarding patient privacy, Alaska health care entities should also be concerned with the Confidentiality of Medical Information rules under state law and the Alaska Personal Information Protection Act .

Together, these laws address Alaska's patient privacy requirements, electronic standardization, security and other privacy requirements that cover use, disclosure and handling of health information, and personal information.

Federal and Alaska state laws have a few differences in the context of patient privacy. First, HIPAA regulations generally only apply to "covered entities," or CEs. These include providers who transmit electronic health care, health care clearinghouses (such as billing companies) and health plans. Alaska law, has a broader scope of coverage. (See chart next page)

Alaska law is also actually more detailed than HIPAA in establishing safeguards for certain types of patient records. When HIPAA conflicts with state laws, HIPAA as the federal law typically preempts the state law, unless the state law is more protective of privacy. (See chart next page)

How does Alaska law define PHI?	How does Alaska law define Covered Entity?	What extra restrictions on disclosure exist beyond HIPAA?	Is there a state law breach or disclosure provision?
No major statute governing PHI beyond HIPAA; privacy is generally addressed in separate statutes governing specific types of entities and conditions.	Restrictions on disclosure for certain entities: EMTs. Alaska Stat. § 18.08.087 Home health agencies. Alaska Admin. Code, tit. 7, § 12.534. Pharmacists. Alaska Stat. § 8.80.315 Community health facilities. Alaska Admin. Code, tit. 7, § 13.130 Nursing homes. Alaska Admin. Code, tit. 7, § 12.890 State agencies. Alaska Stat. § 40.25.120.	Restrictions on disclosure for certain conditions: Substance abuse. Alaska Stat. § 47.37.210 Cancer. Alaska Stat. § 18.05.042 Genetic testing. Alaska Stat. § 18.13.010 Infectious diseases. Alaska Stat. § 18.05.042 Mental health. Alaska Stat. § 47.30.845 Certain insurers must implement an information security program to safeguard confidential information. Alaska Admin. Code, tit. 3, § 26.705.	Not specific to health information, but, for general personal information breaches, the Alaska Personal Information Protection Act Covers: Notice to Consumers in the event of a Breach of unencrypted personal information, if there is reasonable likelihood that harm to the affected individual will result. Alaska Stat. § 45.48.010 (example: SSNs)

Exercise:

Is it a HIPAA or Privacy Violation?

Is it a HIPAA Violation?

Scenario:

1. Hannah, an ER tech at Hospital X is a huge fan of John Legend and Chrissy Teigen. Hannah follows the TMZ Twitter account very closely and has hashtags set for Chrissy.
2. After Chrissy posts on Twitter about having a placental abruption and losing her baby, Hannah sees Chrissy's tweet and retweets it.
3. Hannah's coworker Jude, sees her tweet and reports Hannah for a HIPAA violation.

Is it a HIPAA Violation?

Scenario:

1. Joan, an ER doctor at Hospital X has an Instagram account which she mostly uses to discuss working conditions and the fact that since COVID, the ER always has too many patients.
2. At the end of a particularly busy ER shift Joan posts a video of herself and a nursing colleague talking about working conditions with the busy ER as a backdrop to her Instagram story.
3. Patients in the ER and their family members can be seen in the background of the Instagram story.
4. Joan's neighbor recognizes her cousin and his wife in the background of Joan's Instagram story, takes screenshots of them and shows it to them. Joan's neighbor's cousin complains to the hospital and to the OCR about this situation.

Is it a Privacy or HIPAA Violation?

Scenario:

1. On February 6, 2023, Dr. Darian does a TikTok post on his own account @doctor.darien. He states that on the prior shift while treating a patient, he had a case that reminded him of the CDC update regarding bacterial outbreak in eye drops.

Yes

2. He talks about these eye infections, called pseudomonas, recently cropping up in certain brands of artificial tears and the fact that as of early February 2023 the CDC has identified 55 people as infected with this bacterial infection that is extensively drug resistant.

No

3. He mentions the brand of artificial tears, Azucar that appears to be causing these

Is it a Privacy or HIPAA Violation?

Scenario:

1. The GMA TikTok posts Dr. Darian commenting as an expert about “Demystifying monkeypox 101”

Yes

2. He describes how monkeypox is acquired, common symptoms, and states that it is not an STI.

No

3. He talks about some studies , how long the isolation period should be, and the impact of monkeypox on pets.

Questions?