

## Social Media: What's Hot... What's Not



Joe W DeLoach, OD, FAAO  
CEO, Practice Compliance Solutions

COPYRIGHT 2021 PRACTICE COMPLIANCE SOLUTIONS

1

### Financial Disclosures – Joe DeLoach, OD, FAAO

I Have Received Honoraria From or Served as a Consultant for: (Partial Listing)

- |                     |                    |   |
|---------------------|--------------------|---|
| •Vision Source      | •OfficeMate        | •Essilor of America   |
| •Alcon Laboratories | •Marco             | •Pearle Vision / SNAPP                                      |
| •Carl Zeiss Meditec | •TSO               | •Vision West  |
| •Optos              | •NVision           | •EyeMart Express  |
| •Diopsys            | •Cleinman Partners | •AAO  |
| •Kowa               | •Vision Trends     | •UHCO, RSO, UAB,<br>Berkley, and other optometry<br>schools |
| •PCS                | •Konan             |   |
| •AllDocs            |                    |   |

Over half the state  
optometric  
associations

There are no conflicts or  
disclosures related to any  
of these groups

Practice Compliance Solutions, LLC – President and CEO

COPYRIGHT 2021 PRACTICE COMPLIANCE SOLUTIONS



2

### Communication – What's Hot?

Communication is what's hot!! And it is possibly the most important component of our doctor:patient and staff:patient relationships leading to the success of our practices.

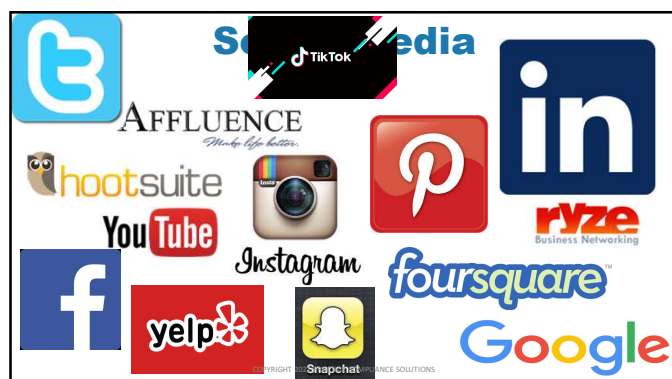
**You may not think about it much – but it is also becoming one of the most dangerous and most regulated aspects of our business lives. It has created unprecedented problems in patient communication, patient privacy and HR management**

3

### Social Media Issues

- Patient **communication**
- **Privacy** of patient PHI
- Human resource **management**
- **Reputation** management

4





5


### Your Patients are Talking about YOU

- Whether you are participating in social media related to your practice or not
- **31 MILLION** text or email messages per minute
- **510K** Facebook posts per minute
- **2.5 MILLION** Snapchats per day
- **80 MILLION** Instagrams per day
- **17,361 individual or company profiles viewed per minute** (that's **YOUR PRACTICE** they are looking at!)

6


 #5 most used app  
 109.5 / ave texts a day  

This is NOT a Millennial / Z-Gen issue!  
 What's on your phone?



7

### Facebook Likes



- According to Dr. Justin Bazan - "Having a large fan base is very important for **marketing** purposes." You create that base through **LIKES**. **Without a strong base** your social media attempts will literally be like talking to a wall."
- According to Dr. Alan Glazier - "**Social Proof**" (**LIKES**) is the most important factor to consider. When someone sees their **friend** "**LIKES**" something, it is a kind of testimonial that the place is legit. The friend is more likely to visit your webpage, **LIKE** it to or at least pay attention to it."

8

### Reviews



- 97% **Positive** / 3% Negative is great
- 100% five star is NOT believable to social media consumers
- You **need the feedback** - you need to know about problems
- The good responses will be **great marketing**
- How you handle **bad reviews** will be **great marketing** – but it is a very slippery slope!!!
- Understand "initiatives" and "personalities" of apps
  - For some, great ratings require financial support
  - Some are a breeding ground for negativism...



9

### Your staff is online too

PROBLEM: In US, average employee spends **1.72** hours of paid time online with **41%** of that time spent on social media sites (ouch!)



AND NOW...



10

### Social Media – may say it all...

Texas Workforce Commission quotes re: Social Media

*"Although social media regulation and technology has improved dramatically, there has been **no corresponding upswing in common sense or decency in society**"*

11

### Here's what you're up against...

*"Employers must realize that social media IS the new news media. The problem is the information comes in so fast that no one, **NO ONE**, can monitor the accuracy or validity of anything posted."*



Mark Zuckerberg  
 Founder & **still** CEO Facebook

12

**Before we start blasting away on Facebook, Twitter, Instagram, ad nauseum....we should look at the rules that govern how we can LEGALLY communicate with our patients**

---

13

## First – know the rules (HIPAA)

- 45 CFR164 522-530
    - All covered entities and business associates are **required by law** to implement measures that “**guard against unauthorized access** to PHI that is being transmitted over **an electronic communications network**”
  - What is an “electronic communications network”?
    - Email
    - Text
    - **Anything involving the internet**
    - FAX?
- 

14

## Communications with Patients

- In general, is **NOT** a great idea unless:
    - Communication is **secured**
    - **Patient initiates** the communication
    - Communication is **generic** to patient base
    - Communication involves marketing, advertising or general health information that is also **generic** to the patient base
  - And end with there is NEVER justification or rationale for posting any PHI on social media, even with **attempted patient authorization** (*can a patient “waive” their HIPAA rights?*)
- 

15

## Three Types of Communication

1. **FROM** the patient
  2. **TO** the patient
  3. **TO a Third Party**  
(anyone OTHER THAN the patient)
- 



16

## Communications FROM the Patient

- The HIPAA Privacy and Security Rules **do NOT apply to communications FROM the patient**. But as soon as the provider receives the email, the information now **must be protected by the provider**.
  - For any communication BACK to the patient from their initial response or any contact initiated by the provider, **refer to next slides**
- 

17

## Communications TO the Patient

- “The Security Rule **does not expressly prohibit the use of:** **email** to communicate with a patient. However, the standards require certain procedures to restrict access, protect the integrity of and guard against unauthorized access to PHI.”
- What are “certain procedures”?  
“**reasonable precautions... equivalent to encryption**”

[www.hhs.gov/ocr/privacy/hipaa/faq/securityrule](http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule)

---

18

## Communications TO the Patient

If you elect to communicate with your patient via email, you have two choices:

1. **Secure the Transmission** - "Equivalent to encryption" – *whatever that is*
2. **Obtain acknowledgement from patient**

We suggest all communications are encrypted. HHS suggests email communication be limited to only **secure patient portal** systems (likely an ultimate rule)

[www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information](http://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information)

19

## Communications TO the Patient

If using **non secure transmission**, required to **inform the patient**:

- The communication **may not be secure**
- The potential **consequences** of that
- Patient **must confirm** they understand the risks and confirm they wish to continue. Does not state HOW they confirm this but anything less than **written authorization** would be foolish

[www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information](http://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information)

20

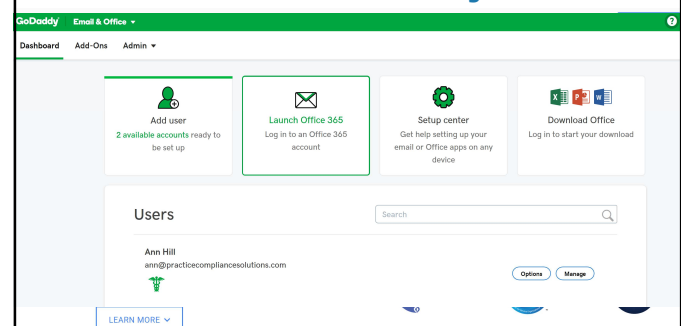
## Communications TO Third Party

- **No stated exception** to the encryption criteria and no expressed authority for the patient to "waive" these security measures. **In fact court rulings to the contrary**
- **Specifically includes text and email communication** (*but not FAX – can't encrypt or decrypt FAX*)
- This is EVERYONE else – **including referral letters!**

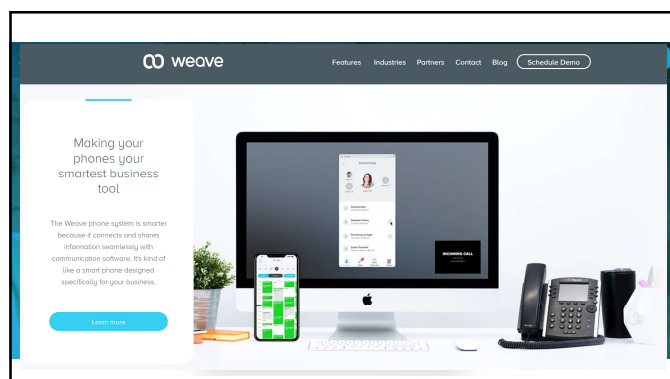
[www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information](http://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information)

21

## Are there secure email systems?



22



23

## SUMMARY ON TEXT / EMAIL

Well maybe we can say that...  
Feb 2017

**Children Hospital, Texas – settled with OCR for \$2.3 MILLION for failure to encrypt text communications with patients**

**And Social Media?**

24



This stuff  
sucks....

COPYRIGHT 2021 PRACTICE COMPLIANCE SOLUTIONS



25

## Social Media

### Six Social Media Situations for Health Care Practitioners *(we'll go over each)*

1. Communications with patients on social media
2. Communications on blogs / websites
3. Social media for background checks, "looking at" current or potential employees
4. "On duty" (during business hours) employee communication on social media
5. "Off duty" (outside of business) employee communications on social media
6. Employer liability for employee postings on social media

26

## Responding to reviews / posts

Debated....three potential answers:

1. **Don't do it** – call the patient to discuss / resolve
  - Technically best answer...
2. **Answer in NON-SPECIFIC terms** then call the patient to discuss / resolve
  - Probably OK answer – good recommendation
3. **Go off on them** – they started it
  - You might as well get your checkbook out

27

## So lot's of opinions - any of them right?

While many practice management consultants strongly advise providers to respond to patient postings on social media, HIPAA rules may dictate otherwise. This specific issue was addressed by HHS in 2020. [Here is how it went down....](https://www.hhs.gov/about/news/2019/10/02/dental-practice-pays-10000-settle-social-media-disclosures-of-patients-phi.html)

The case appears to make it clear HIPAA looks at provider response to online posts in a very negative manner (\$10,000 fine) unless the provider has patient authorization.

<https://www.hhs.gov/about/news/2019/10/02/dental-practice-pays-10000-settle-social-media-disclosures-of-patients-phi.html>

28

## Can I post pictures of patients?

What about those cool new frames? That cute kid behind the refractor during their first eye exam?

**Sure....IF**

- The patient authorizes it (or does it themselves)
- You don't make any comments about **PHI – even something benign** like:  
"Look how Mary's new lenses aren't so thick any more!"

29

## Can I post cases on blogs?

Blogs have great points – **BUT**

Without patient authorization – **you CANNOT post anything that could POTENTIALLY identify the patient**

- The obvious – names, patient numbers, SS#, DL#, address, occupation, too much history information – and the list goes on and on. HIPAA describes a violation as **"any combination of information that could potentially identify"**
- Evidently not so obvious – identifying pictures. Definitely full or partial facial photos but could also include **"any mark, irregularity or pathology that could identify the patient"**

30

## Posting on blogs

- Often scoffed at by blog participants – but already have privacy cases on this.
- California Supreme Court ruled that the simple “act of posting” is a violation even if human eyes never see the post.
- The argument of “a private blog” does NOT hold water. **Nothing on the internet is private, period!**
- The question of patient authorization is still up for grabs. It is likely a good protection but not the safest action (*“I didn’t know...”*). Safest action is do not post anything that could even POTENTIALLY identify a patient.

31

## Using social media to people”

Austin, Tx  
September 2019

- This may include non-private background checks; non-private credit checks; evaluating folks based on Facebook page - comments, likes, photos; evaluating folks based on Twitter postings
- **This is a VERY bad idea** – because:
  - The information is often incorrect and not verifiable (*remember, we are in the age of “fake news”*)
  - Judgement based on LEGAL off duty behavior is considered DISCRIMINATION (again, get your checkbook out)
  - Employers can be held liable for any decision regarding a new or existing employee based on this information, **even if the information was posted incorrectly by the employee, applicant or anyone else!**

Repeat – bad idea. Don’t do it! (if you do don’t admit to it!)

32

## But Joe...common sense says how to act on social media!!!

### 3/2022 – Popular OD Blog

*So for me I do all of the pre-op and post-op care for my LASIK patients. I collect the full fee upfront and pay the OMD after the procedure. I’m there in the procedure room with the patient as well, and I’m doing the post-op evaluation at the facility.*

*This patient asked me if it was OK for her to smoke weed today when she gets home.... Never had a patient asked me that before.*



No...I blocked out the faces and name!!!

*I don’t think I would do that – would be concerned about increased dry eye*

33

## Social Media Employee on duty vs off duty communication

### DEFINE:

**ON DUTY communication** – posting through the internet during time the employee is “on the clock”. The posting can be performed using the employer’s equipment or the employee’s equipment – and this may make a difference!

**OFF DUTY communication** – posting through the internet during time the employee is NOT “on the clock”

34

## Social Media Employee on duty vs off duty communication

### The Most Common Problems

- Inefficient use of work time (*remember, 1.72 hours per day!!!*)
- Harassment (other employees or even patients)
- Endorsements
- Pornography (*oh yeah, PCS had to deal with this with a client!*)

35

## Social Media Employee on duty communication

Employers have every right to monitor employee activity on the internet when such communications are:

- Made during the hours employee is on the clock
- Made on equipment the employer owns or manages
- Is work related – and to some degree when the activity is not work related (*careful!!*)

36

## Social Media MONITORING...BE CAREFUL!

Monitoring activities must be:

- Legal in your state (*varies per state – why state-specific HR is imperative*)
- Based on written office policies
- Uniformly applied to all employees
- Authorized by the employee – not a legal requirement in most states but is in Washington (*“two-party consent” state*)!
- Based on some rational reason – surreptitious monitoring is definitely illegal

37

## Social Media Employee off duty communication

This one is far trickier!

The National Relations Labor Board allows employers to monitor off duty employee postings as long as the activity might directly effect:

- Fellow co-workers
- The employer’s business
- The employer’s patients, customers or other clients
- Employer’s “trade secrets” – poorly defined

38

## Social Media Employee off duty communication

The problem – poor clarity:

- The biggie – NLRB states employee’s 1st amendment rights must be protected. Again, how far does that go?
- “Directly effects” poorly defined
- Per NLRB...Employees have to right to post anything related to the **“conditions of their employment”** – also loosely defined but definitely includes working conditions, compensation, hours, benefits, **demeanor of the employer**. And there is significant leniency regarding the “accuracy” of the post!

39

## How Far Can An Employee Go? Hold on to your hats...

An employee gets a somewhat negative annual review that does not result in a pay increase. They are very upset and post on Facebook:

***“ABC Company is is horrible place to work. Mr. ABC is a cheap, fatso piece of s#\*%! who doesn’t care about anything but his pocketbook”***

NLRB declared the post is allowable as the profanity and comments about the employer were related to their “working conditions” and made during an emotional outburst that was the result of their disappointing review.

**AND SEVERAL SIMILAR DECISIONS SINCE THIS ONE! BUT LET’S ALL AGREE THIS IS TERRIBLE WAY TO ACT!**

40

## Social Media - Summary Employee on and off duty communication

***Monitoring for ANY reason in ANY situation can be tricky!***

NLRB states employees have a right to “reasonable protection of their privacy” – again, poorly defined. The courts generally rule in favor of employee “rights” on this – be very careful!

41

AHHHH!!! But can you tell us something REALLY important?



**Turtles can breath through their butts**

COPYRIGHT 2021 PRACTICE COMPLIANCE SOLUTIONS


42



## Social Media Employer Liability for Employee Actions

- HIPAA holds the employer liable for the actions of staff unless they have established HIPAA privacy and security regulations and have trained their staff
- Employers have liability for the postings of an employee that are damaging if the posting is deemed to be an endorsement representing the employer (*and most are considered as such*)
  - Back to tricky again – poorly defined, potential infringement of 1st amendment rights
  - Are we really going to take it this far? Likely to also be determined in courts

Refer to SEC Release No. 34-58288

43

## And life is just not fair sometimes!

All these “protections” do not flow both ways

- Communications Decency Act of 1996 - a business owner may not claim damages for against network hosting or social media site for not monitoring negative comments – including accuracy (essentially these companies are immune from actions resulting from communications by 3<sup>rd</sup> party). Currently being challenged but no change yet!
- Courts have ruled that in certain situations employers may be held liable for the actions of their employees on social media even when such actions are performed “off duty”

44

## Social Media – Most Important Solution

- At a minimum, employers should include a social media policy in their employee handbook.
- ONE PERSON controls the business’s social media
- The main policy should be **“Your job comes first”**
- Like other HR policies, employers must oversee their business and apply policies in a fair and consistent manner for all employees

45

## Social Media – Recommended Policies

Company postings should NEVER contain:

- Confidential business information (usually financial)
- Discriminatory, defamatory, disrespectful or derogatory statements about other employees, patients or any client of the practice
- Any illegal, sexual or unprofessional information
- Comments of a personal or emotional nature such as politics, religion and the like (*Politics?? That is a HOT issue!*)
- False, unconfirmed or misleading information

46

## Social Media – Recommended Policies

Without approval, company postings should not contain:

- Endorsements of or references to products or services
- Material or information not approved by the employer
- Material copied from another source unless accuracy verified and typically only with consent
- Information not related to the operation and purpose of the business

47

## Social Media – Recommended Policies

Without approval, **personal** postings should not contain:

- Endorsements of products or services except personal opinion – disclaimers recommended
- Confidential business information (usually financial)
- Discriminatory, defamatory, disrespectful or derogatory statements about other employees, patients or any client of the practice
- Items that could be damaging to the employer’s business

48



### MOST IMPORTANT CONCEPT

What goes on social media STAYS on social media – *forever*. Be a respectful, rational **adult** and all these silly laws can go away!

---



49

MAY YOUR LIFE BE  
AS AMAZING AS  
YOUR SOCIAL MEDIA  
PROFILES MAKE IT  
SEEM.

**Thank  
You!**

**Have a  
Great 2022**

[joe@pcscomply.com](mailto:joe@pcscomply.com)

---

50