OBER | KALER
Attorneys at Law

www.ober.com

Social Media, Health Care Privacy and Your Employees:

7 Tips to Avoid HIPAA Violations and Employee Claims

Welcome

- Many healthcare providers are establishing and managing their own social networking activities for patient communications and, increasingly, marketing.
- The intent of this webinar is to discuss issues relating to the risks of social networking by members of the workforce of covered entities and business associates.
- We will define social networking and discuss the technology of each, with specific reference to HIPAA risks.
- Covered entities and business associates can attempt to bar the use of social networking by members of their workforce
  - Using technology provided by the covered entity or business associate, or
  - Using the employee’s own technology’
- Our premise is that covered entities and business associates should focus on developing a comprehensive social media policy and aggressively educating members of their workforce on the implications of HIPAA on the use of social media.
- Establishment of a HIPAA social media policy must include consideration of employment law as well as HIPAA.

What We Will Cover Today

- The technology
- A balancing act
- Scenarios
- When it goes badly
- Intersection between HIPAA and HR
- What is on the horizon
- Your questions

Speaker Information

Jim Wieland

jbwieland@ober.com | 410.347.7397

Sarah Swank

seswank@ober.com | 202.326.5003

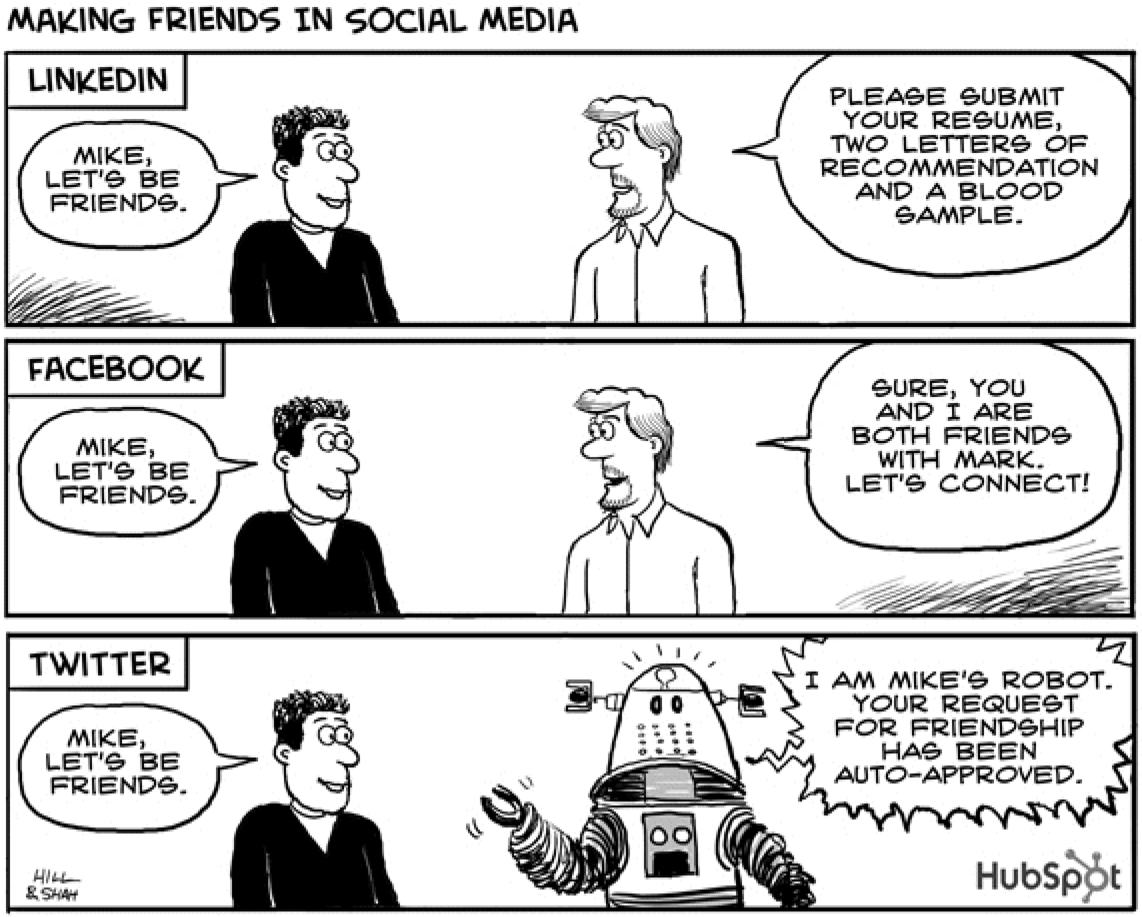
Carla Murphy

cnmurphy@ober.com | 410.347.7680

Josh Freemire

jjfreemire@ober.com | 410.347.7676

Now Let’s Get Started . . .


MAKING FRIENDS IN SOCIAL MEDIA
LINKEDIN
MIKE, LET'S BE FRIENDS.
PLEASE SUBMIT YOUR RESUME, TWO LETTERS OF RECOMMENDATION AND A BLOOD SAMPLE.
FACEBOOK
MIKE, LET'S BE FRIENDS.
SURE, YOU AND I ARE BOTH FRIENDS WITH MARK. LET'S CONNECT!
TWITTER
MIKE, LET'S BE FRIENDS.
I AM MIKE'S ROBOT. YOUR REQUEST FOR FRIENDSHIP HAS BEEN AUTO-APPROVED.
HILL & SHAH
HubSpot

TIP 1: Understand the Technology

- “Social Media” is an umbrella term that encompasses several different types of technology
- These different technological types provide a combination of media storage, display, and communication applications
- Each allows a single person to communicate to a broadly identified group
- Different technologies pose different risks, and must be addressed thoughtfully
- Policies and education should be focused on the communication made, not the brand name

TIP 1: Understand the Technology

- Common social media applications (and much heard buzzwords) include Facebook, LinkedIn, Twitter, Weblogs (“Blogs”), websites (including photo sharing sites), Instant Messaging, and “Texting.”
- Each technology operates slightly differently, though some share a similar technological structure (Such as Facebook and Linked In, for instance).

TIP 1: Understand the Technology

Facebook

- Ubiquitous photo, messaging, and mail service
- Technology similar to that in MySpace, LinkedIn, Sales Force Chatter and other, similar sites
- 750 million users and growing
- Personal information
- Connections by consent
- Updates pushed to “friends”
- Messages – mail, chat, the “Wall”
- “Tagging” photos and locations in other friend’s photos.
- Additional applications and add ons – games, surveys, groups

TIP 1: Understand the Technology

Facebook

- Users have a wide variety of privacy functionalities and can maintain high level of privacy
- Newer or more naïve users may not be aware of privacy functions, risks
- Privacy functionalities are constantly in flux.

TIP 1: Understand the Technology

Facebook

- User information is stored and controlled centrally.
- User controls cannot override corporate decisions – posted information is “out there” forever.
- Posted information can be stored or saved by other users – especially, pictures, for example.
- Technology is mobile, ubiquitous, and free – anyone with a smart phone can access Facebook, post photos, and communicate in real time.
- Accounts can be faked or hacked.
- Both Facebook and third party application providers collect personal information to share with advertisers and other third parties.

TIP 1: Understand the Technology

Twitter

- Short bursts of text, links, or pictures to thousands, if not millions, of “followers”
- Messages limited to 140 characters (“Tweets”)
- Tweets are sent through the internet, but may originate from mobile phone applications or even text messaging services
- Applications add the ability to share links, re-post others’ “tweets” and to share photos

TIP 1: Understand the Technology

Twitter

- Iphone applications for Twitter photos – TweetDeck, Echofon, Tweetie, Twitfile and Twitterrific – ubiquitous tech.
- Data is centrally stored and is not user controlled. Private messages may be sent, but default is public.
- Information sent is forever “out there” and may not be recalled.
- Shared photos may used or sold to another entity (TwitPic).
- Accounts may be faked or hacked, and Twitter openly shares user information with third parties.
- FTC brought action to force Twitter to improve its security, settled in 2010.

TIP 1: Understand the Technology

Websites

- Personal websites, or common photo sharing sites (Flickr, Snapfish)
- Content is controlled by user (uploaded text, movies, pictures)
- Publicly available as default
- Some photo sharing sites have functional privacy controls, but generally default to public availability.
- Personal websites may be shut down by a user, but information that is made available on the internet may always be copied and may be stored.

TIP 1: Understand the Technology

Blogs

- Web Logs, or “blogs” allow users to post an online multi-media journal on a specific topic or topics of general interest.
- May be operated on a personal website or blog hosting site
- Content is almost always public.
- Hosted content is subject to hosting companies terms of use, may not be entirely controlled by poster.
- Greater control of user, but it is still subject to copying and storage
- Blogs may be hacked or faked

TIP 1: Understand the Technology

Instant Messaging

- Permits two users to communicate in real-time via short typed messages aka “chatting”
- Hosted internally or externally –security levels can vary widely
- Chat transcripts may be stored
- Frequently available for free on smart phones and similar web enabled devices

TIP 1: Understand the Technology

Text

- Short Message Service or SMS
- Permits users to send short messages over a dedicated data channel available to all cellular devices.
- Inherently insecure
- Texts are generally stored on a central server of the cellular provider (or more than one) as well as on both the sending and receiving devices.

TIP 2: Pay attention to Old Problems

Identify Risks

- All social media technology is simply a means to communicate.
- The familiar HIPAA rules apply to social networking; except for TPO and other more limited exception, patient authorization is required for uses and disclosures of Protected Health Information. Even demographics are considered to be PHI.
- Depending on the technology used, and the audience targeted, breaches could be widespread and difficult to trace or investigate or they could be discrete and more manageable.
- “Communication” is the key – protected health information that finds its way onto social media is being communicated, typically without authorization, and likely constitutes a breach.
- Company policies should reflect the risk inherent in each type of technology.

TIP 2: Pay attention to Old Problems

Identifying Risks

- All Technology is not the same
- Investigations will be necessary
- Technology that permits users to protect information and limit audience are, in many ways, more secure
- Facebook, in this respect, poses less of a threat than a publicly available web site or tweeted photo
- Degree to which privacy controls can mitigate breaches depends heavily on the degree to which they are utilized

TIP 2: Pay attention to Old Problems

Example

At a birthday party for one of the nurses on the floor, an employee snaps a photograph of nurse A, B, and C who have worked together for years. In the background, unbeknownst to the photographer, a white board lists that Patient Z, a locally well-known television personality, is in room 123 awaiting a procedure and is HIV positive. Nurse A posts the photo on her Facebook page, Nurse B tweets it to her friends, and Nurse C uploads the picture to Flickr and links to it on her blog on nursing care. The hospital is informed when the photo appears on a local celebrity news site. While unintentional, a clear breach has occurred.

TIP 2: Pay attention to Old Problems

Nurse C = Photo Share + Blog

- The photo is probably publicly available and may be viewed and copied by an unlimited number of people.
- It may possible to tell how many times the photo was viewed.
- While the nurse can control the photo by removing it or limiting who may view it on Flickr, she has rendered that protection meaningless if she direct links to it in her blog.
- The nurse can remove the photo and the link herself to halt the continued display, but
- Even after the photo and link are removed, copies may exist.

TIP 2: Pay attention to Old Problems

Nurse B = Twitter

- When Nurse B tweeted the photo, she granted another company the right to use and/or sell the image (TwitPic).
- She may be able to delete the picture from her own Twitter feed, but she can not "get it back" from the company servers.
- Similarly, she cannot get it back from those who "re-tweeted" it, or copied it, and she cannot tell how many people saw it, or who copied it.
- Assuming that the tweet was general in nature, it defaulted to a public setting and was available to all while it was posted.
- Case in point – Representative Anthony Weiner (whose tweets were NOT public, but became so rapidly)

TIP 2: Pay attention to Old Problems

Nurse A = Facebook

- Nurse A’s posting may be a very limited disclosure.
- Photo may have only been available to her friends that also work in the hospital or a similar sub-group.
- If no controls are used, however, the photo may have been publicly available – all friends, or even public.
- She may delete the photo from her account, but friends may have copied it or stored it in the interim.
- Further investigation will be necessary to determine the extent of the breach from Nurse A’s posting.

TIP 2: Pay attention to Old Problems

Risk Takeaways

- The use of social media is multi-channel – too much tech to list, and more developed every day
- All it takes is a phone and a moment to create a breach
- Breaches can move alarmingly fast – one tweet can reach thousands instantly
- Employee education is more practical than prohibition
- Educated employees can mitigate and avoid risks – but you must know your workforce, including what they need to know

TIP 3: Know Your Workforce

The technology is here to stay

- Your workforce uses it . . .
  - On your computer system
  - On a smart phone
  - Away from work

"Must dash ... I want to spend some time on my social-networking websites."

TIP 3: Know Your Workforce

Everyone is using it . . .

TIP 3: Know Your Workforce

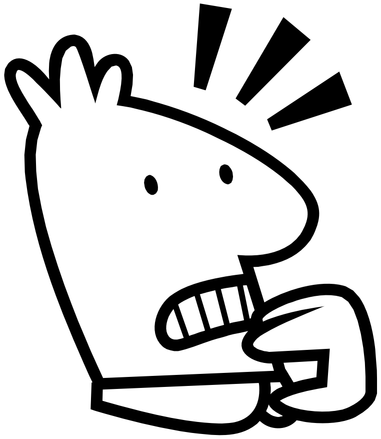
Social Media can be GREAT!

- Branding
- Communication tool
- Creates a sense of community
- PR
- Fundraising
- Establish organization as expert or leader

TIP 3: Know Your Workforce

Are You Afraid?

- Loss of productivity
- Privacy issues
- Loss of control
- Employment issues
- Unions



TIP 3: Know Your Workforce

Who is your Workforce

- Workforce means
  - employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
- You are responsible for your workforce under HIPAA
- Even on social media . . .

TIP 3: Know Your Workforce

What About Others?

- You are not responsible for patients, family members, visitors or others under HIPAA
- But . . .
  - You invite others to post then you may be liable
  - Important to discuss volunteer nature of posting

Example: Marketing sets up a new site for moms

TIP 3: Know Your Workforce

Example 1

Physician takes a picture with her smart phone of a patient in OR for “treatment purposes”.

What if it was not for treatment purposes?

He then sends a text with the picture to his office staff.

What if he posts it on Facebook, instead?

TIP 3: Know Your Workforce

Example 2

New dad takes picture of nurse to remember the wonderful care and posts it on Facebook.

What if there are other babies in the background.

What if the nurse does not consent.

What if the care was not so wonderful . . .

TIP 3: Know Your Workforce

Example 3

Home health nurse gives updates on status using text.

She tweets regularly about her experience as a nurse. Does it during work hours sometimes.

Includes comments related to patient visits.

Is fired and writes about clinical policies of management.

TIP 3: Know Your Workforce

Ripped from the Headlines

- Sharing Photo Of Gunshot Wounds Gets Hospital Staffers Fired, July 22, 2011
- Clinician at Connecticut's Hospital of Saint Raphael Texts Photo of Murdered ER Patient, July 26, 2011
- When Facebook goes to the hospital, patients may suffer, August 8, 2010

TIP 3: Know Your Workforce

Your Whole Workforce Must Work Together

- Leadership
- Nurses
- Physicians
- Clinical staff
- Support staff
- Fundraising
- Marketing
- PR

TIP 3: Know Your Workforce

Workforce Checklist

✓Do they know the organizations philosophy

✓Do they understand your policies, code of conduct

✓Don’t underestimate need for retraining

✓Do they know where to go with an issue

TIP 3: Know Your Workforce

Workforce Checklist

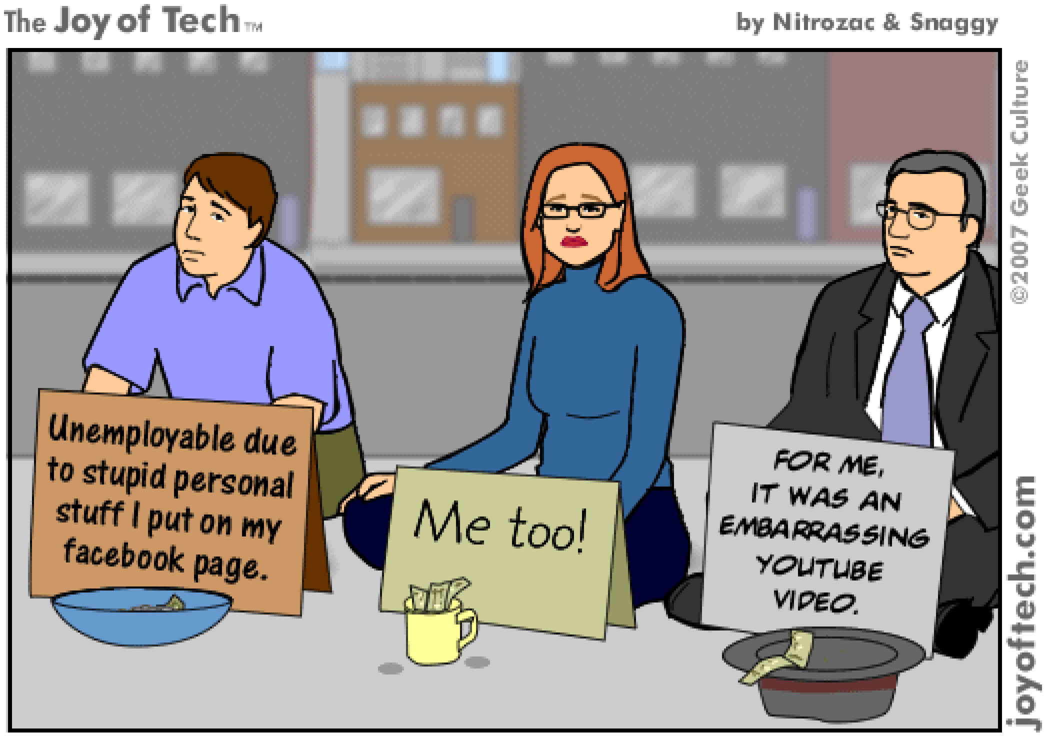
✓Sign confidentiality agreements

✓Use of your computers for social media

✓Use Smart phones and other devices as part of the job vs. person use

✓Signage up about photography and cell phones

TIP 3: Know Your Workforce


The Joy of Tech™
by Nitrozac & Snaggy
Unemployable due to stupid personal stuff I put on my facebook page.
Me too!
FOR ME, IT WAS AN EMBARRASSING YOUTUBE VIDEO.
©2007 Geek Culture
joyoftech.com

Signs of the social networking times.

TIP 4: Investigate, Mitigate and Discipline

- Given: In the examples given above (Nurse A, B and C), there is a breach of unsecured Protected Health Information, requiring notification of the individual involved.
- In most situations, the breach will be of a single individual, or at least of less that 500 individuals, mitigating somewhat the cost and reputational damage of the incident.
- In the event the information that is posted included personal information, Social Security Number, Drivers License Number, or bank or credit card information, state consumer protection laws may, separately from HIPAA, require notification of individuals and, in man states, state regulatory agencies.
  - California includes “medical information”, broadly defined, in its consumer protection laws requiring individual notification.

TIP 4: Investigate, Mitigate and Discipline

Mitigation

- The challenge is mitigation of the of the effect of the disclosure.
- The answer depends on the social media that are involved, but every effort must be made, and documented to have been made.
- Take down of the Protected Health Information is the goal.
- Reality is that once something is posted on the internet, it may never go live forever. Information can be disseminated in a variety of ways - copied, emailed stored on line and off-line

TIP 4: Investigate, Mitigate and Discipline

Terms and Conditions of most social networking sites grant the site broad rights to posted data:

- For example, Facebook T & C provide as follows:
  - You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
  - For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: **you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.**
  - When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. **However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).**
  - When you use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Privacy Policy and Platform Page.)
  - **When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture).**
  - We always appreciate your feedback or other suggestions about Facebook, but you understand that we may use them without any obligation to compensate you for them (just as you have no obligation to offer them).

TIP 4: Investigate, Mitigate and Discipline

Mitigation

- Terms & Conditions notwithstanding:
  - Determine the rights of the workforce member that made the posting and request that he/she remove the posting;
  - Contact the social media site, cite HIPAA and request assistance in removing the material;
  - Make whatever efforts are possible to trace and remove secondary postings; and
  - Use the posting as a teaching opportunity to prevent further violations.

TIP 4: Investigate, Mitigate and Discipline

Investigation

- Discovering the issue
- Different type of investigation – not always patient driven
- Coordination of HR and Privacy Officer
- Interview witnesses and workforce members
- Not as likely to speak or write to the patient or personal representative during investigation
- Consider reporting obligations and respond appropriately
- Respond to government or patient, as appropriate

TIP 4: Investigate, Mitigate and Discipline

Discipline

- Factors:
  - Harm to the patient or covered entity
  - Intent
  - Lack of training
  - Previous violations
  - Severity of the incident
- Be Coordinated
- Be Consistent

TIP 5: Develop a Social Media Policy

- Why Do You Need One?
- Govern how employees use social media in and out of the workforce
- To protect confidential information and prevent improper use of social media
- To provide protection in litigation
- To outline disciplinary procedures

TIP 5: Develop a Social Media Policy

- How Do You Create One?
- Know and evaluate your risks
- Tailor to company culture & approach to technology

TIP 5: Develop a Social Media Policy

- What Should Be Included?
- Description of social media & purpose.
  - Define social media.
  - Explain no reasonable expectation of privacy in any social media communications (including real time).
  - Explain communications are not secure.
- Address use of social media on company time and use of company equipment
  - Business related use only?
  - Limited personal use? On assigned computers?

TIP 5: Develop a Social Media Policy

Elements of a HIPAA Social Media Policy

- Distinguish between use of covered entity provided technology and personal technology
- Dovetail with employment policies
  - Define “social media”: online forums, blogs, microblogs, wikis or vlogs (e.g., Facebook, LinkedIn, MySpace, YouTube, Twitter, health pages and blogs, media sites or similar types of online forums).
  - Make it clear that the same policies and procedures that apply to uses and disclosures of Protected Health Information in day-to-day work apply with equal force to uses and disclosures of PHI in the context of social media.

TIP 5: Develop a Social Media Policy

Elements of a HIPAA Social Media Policy

Emphasize that social media do not create a new type of communication with new or different individual responsibilities. Social media simply create new means to communicate. If you wouldn’t say it in a crowded hospital elevator, don’t say it in social media.

- State clearly that it is the policy of the covered entity that Protected Health Information of patients is not to be posted on social media by work force members.
- Key is to provide examples of Protected Health Information that are relevant to Social Media:
  - Photographs of, or including a patient, are Protected Health Information if taken in the hospital, since the photograph may directly or indirectly identify the individual’s health care condition
    - A patient may be inadvertently included in the background of an otherwise innocent photograph in some treatment context.
  - A patient may be identifiable from a discussion and context: “Guess which rock star we saw in the Emergency Room last night? He must have spent the entire time before his concert drinking! Did we have a problem!” This is Protected Health Information

TIP 5: Develop a Social Media Policy

- Prohibit Disclosure of Confidential Information
  - Specify “No disclosure of member/patient identifiable information of any kind – even if the individual is not identified by name”; provide examples.
  - Specify no disclosure of trade secret information.
  - Reference other company policies – confidentiality, electronic use, cellular phone policies.

TIP 5: Develop a Social Media Policy

- Prohibit discriminatory/harassing statements about co-workers, current and past employee and patients.
  - Reference company anti-discrimination and anti-harassment policies.
- Prohibit defamatory comments regarding the office, employees, patients, services.
  - Specific that the policy will be applied and construed in accordance with Section 7 of the National Labor Relations Act (“NLRA”) - Protected Activity exception.
  - Carve out whistleblower protection to explain that employees can voice good faith concerns about a law or regulation that may have been violated, company conditions affecting public health and safety, and suspected privacy and securities fraud breaches.

TIP 5: Develop a Social Media Policy

- Section 7 of the NLRA provides:
    - Employees shall have the right to self-organize, to form, join, or assist labor organizations, to bargain collectively . . . <u>and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid and protection</u>.
- This means you can't prohibit employee posts that can be seen as an attempt to improve working conditions. For example,
    - Posts that criticize operations impacting employees.
    - Posts discussing wages, hours, & other working conditions.
    - Posts that disparage supervisors or management
- Section 7 has been interpreted very broadly and the Board is taking an aggressive approach towards work rules and policies, including social media policies, which <u>might</u> be interpreted to restrict employee's right to engage in concerted activity.
- Effective November 14, 2011, employers are required to post notices in workplace informing workers of their rights under the NLRA.

TIP 5: Develop a Social Media Policy

- *American Medical Response of Connecticut*, Case No. 34-CA-12576
  - Employer terminated EMT employee for criticizing her supervisor on Facebook. The post was made from the employee's home computer and some of her co-workers saw the post and joined in, which led to the employee posting further negative remarks about her supervisor.
  - The Board's complaint alleged the termination violated the NLRA by restricting the employee's right to discuss the terms and conditions of her employment. It stated that it was a "straight-forward case," and that whether it takes place on Facebook or at the water cooler, it was employees talking jointly about working conditions, in this case about their supervisor, and they have a right to do that."

TIP 5: Develop a Social Media Policy

- *Hispanics United of Buffalo*, Case No. 3-CA-27872.
  - Employer terminated five employees for griping after hours on Facebook about their jobs, one of their managers and some of their more challenging social service clients.
  - The Board held that “explicit or implicit criticism by a co-worker of the manner in which they are performing their jobs is a subject about which employee discussion is protected.”
  - The Board further explained “Employees have a protected right to discuss matters affecting their employment amongst themselves,” and it was “irrelevant . . . that the employees were not trying to change their working conditions and that they did not communicate their concerns to” their employer.

TIP 5: Develop a Social Media Policy

- What Should Be Included?
- Advise of risks of copyright, patent or trademark infringement.
- Require disclosure and disclaimer if employees endorse company or services.
  - Disclosure – Federal Trade Commission ("FTC"), Truth In Advertising requirements.
    - "I work for Dr. X and think she is the best."
    - My employer, ABC Company, gave me these great products to try."
    - FTC "Frequently Asked Questions" : http://www.ftc.gov/bcp/edu/pubs/business/adv/bus71.shtn
  - Disclaimer – Personal Views
    - "Postings on site are my own and do not represent the Company's opinions, beliefs or positions."

TIP 5: Develop a Social Media Policy

- What Should Be Included?
  - Violation of the policy may result in disciplinary action, up to, and including termination.
  - Reporting Requirements
  - Notify supervisor or privacy officer of policy breach

TIP 6: Don’t Be a Snoop

- Employers most commonly use social media to investigate applicants and to monitor employee use of social media.
- Advantage of reviewing social media is knowledge.
  - Future Employees
    - misrepresentation of qualifications
    - breaches with regard to former employers
    - inappropriate posts
    - discriminatory/harassing comments
  - Current Employees
    - misrepresentations with regard to ability to work
    - disclosure of confidential information
    - inappropriate posts
    - discriminatory/harassing comments

TIP 6: Don’t Be a Snoop

- Disadvantage of reviewing applicant and employee social media is knowledge.
  - Discrimination Concerns.
    - Race
    - Religion
    - National Origin
    - Sexual Orientation; Gender Information
    - Age
    - Disability
    - Pregnancy/Marital Status
    - Military Plans

TIP 6: Don’t Be a Snoop

- Another disadvantage of reviewing applicant and employee social media is that such review can lead to privacy-related tort and statutory causes of action.
  - Tort Privacy Causes of Action
    - Intrusion upon the plaintiff’s seclusion or solitude. Generally, an employee must allege: (1) an intentional intrusion, physical or otherwise, (2) upon the plaintiff’s solitude or seclusion or private affairs or concerns, (3) which would be highly offensive to a reasonable person. An employer may defend itself by establishing that the employee did not have a reasonable expectation of privacy.

TIP 6: Don’t Be a Snoop

- Stored Communications Act: 18 USC § 27010
  - To the extent an employer requests or requires an employee’s social networking password or login (or uses such information without authorization), a review of social media sites may violate the Stored Communications Act, which prohibits intentional unauthorized access to stored electronic communications.
  - In *Pietrylo v. Hillstone Restaurant Group*, 2009 WL 3128420 (D. N.J. 2009), a federal jury found in favor for two managers who started a private, invitation-only, password protected MySpace group for their co-workers to “shit talk,” where their employer had requested password from one of the employees and then accessed the site.

TIP 6: Don’t Be a Snoop

- Federal Wiretap Act, as amended by Electronic Communications Privacy Act, (18 U.S.C. 2510).
    - The federal Wire Tap Act makes it unlawful intentionally to intercept an oral wire or electronic communication using an electronic, mechanical or other device.
    - In *United States v. Szymuskiewicz*, 622 F. 3d 701 (7th Cir. 2010), the court affirmed a criminal conviction of IRS worker pursuant to the Wiretap Act for setting up auto-forwarded feature on his boss’s e-mail account without his boss’s consent.

TIP 6: Don’t Be a Snoop

- Employers can take several steps to minimize legal exposure with regard to review of employee social media.
  - A Social Media policy for employees explaining they have no reasonable expectation of privacy in social media posts is crucial.
  - Consider obtaining a stand alone consent form from employees, as well as a consent form from potential employees permitting social media searches.
  - Consider drafting a policy for management to address how to run searches on potential and current employees and how to handle information received.
  - Consider using a non-decision maker to run the searches and report only relevant information.
  - To avoid potential liability, employers should not pose as a co-worker to friend another employee. Employers also should not attempt to get break into password protected or private sites.
  - Be consistent. If you choose to run a social media search on potential applicants, do not select a few haphazardly, but search all candidates in the same manner. Also be consistent with regard to how and when you monitor employee use.
  - Document information used to disqualify candidate or discipline employee.

TIP 7: Track the Moving Target

- GOA
- AMA guidelines
- FDA proposed rule
- HIPAA changes
- Quickly evolving technology
- Regularly review policies!

Questions?

Contact Information

Jim Wieland

jbwieland@ober.com | 410.347.7397

Sarah Swank

seswank@ober.com | 202.326.5003

Carla Murphy

cnmurphy@ober.com | 410.347.7680

Josh Freemire

jjfreemire@ober.com | 410.347.7676