

SOCIAL NETWORKING AND THE MEDICAL PRACTICE

GUIDELINES FOR PHYSICIANS, OFFICE STAFF AND PATIENTS



The usefulness of online social networking is undeniable and it's no surprise that physicians are embracing it. But... these tools present a minefield of legal and professional hazards for medical professionals who don't take the utmost care in how, what and where they post.

- E. Berkman, Massachusetts Medical Law Report

This memorandum was developed for general informational purposes only. It is not meant to be a comprehensive guide, nor should it be construed as authoritative legal advice. This memorandum was developed by the OSMA Legal Services Group with the assistance of Anjenette Santelli, Capital Law School Intern.

Surveys show that 35 percent of American adults have a profile on a social networking site. Seventy-five percent of Facebook users admit to checking their Facebook at work, on company time and company-owned equipment. In 2004, more than 10 percent of employees spent more than half of a day on email (86 percent of which is personal), and more than one in five employers (21 percent) had employee email and instant messages subpoenaed in the course of a lawsuit or regulatory investigation. One hundred percent of information placed on the Web is never really "erased" completely (Pew Internet Project, 2008).

Times have changed. Companies embrace social media to market products and services, and the healthcare field is no exception. Hospitals such as Kaiser Permanente[®] and the Mayo Clinic[®] are utilizing social media platforms for the benefit of patients, employees and practitioners.

While the growing popularity of social media use is mind-boggling (for example, 56,796,060 Facebook users in March of 2009, and 114,190,780 users in March of 2010), the increase in legal and ethical concerns surrounding social media use are overwhelming, fluid and unclear. Here is a roadmap to help guide your course.

IT IS ONLY A RIGHT TO WRITE.

The 'right' to express yourself on a social networking page does not mean freedom from consequences. Remember, you are just as accountable for what you write as you are for what you say, and not surprisingly, the same rules apply to both. Consider the following scenario:

- *A physician shares a general narrative of a recent patient communication on his personal Facebook page, or on a medical-oriented page, like Sermo.*
- **Go ahead:** If the information that is shared is generic enough that nobody can identify a patient in the course of reading (Berkman, Massachusetts Medical Law Report, Social Networking 101 for Physicians, 2009), the post is permitted and is a valuable tool for physicians to share information and skills with other physicians faster than ever before.
- **Stop and Think:** Edited articles in peer reviewed publications are not instantaneous. Publishing a status update on Facebook takes seconds.

What does this mean: The easier it is to publish something, and the less peer review there is, the more opportunities there are to make mistakes.

What to do: Be mindful of the laws and regulations that apply to everyday work, as a physician, an employer or an administrative assistant and create office policies accordingly. For example, require posts on business-hosted blogs to be proofread by a peer before being published. The laws that apply in person will apply within any social media. Some examples include:

- **Title VII of the Civil Rights Act** – prohibits discrimination based on race, color, sex, national origin or religion. This federal law covers private employers, state and local governments and educational institutions with at least 15 employees. Protections have been extended to include discrimination on the basis of pregnancy, sex stereotyping and sexual harassment.
- **Americans with Disabilities Act of 1990 (ADA)** – prohibits employment discrimination based on disability. Employers may not inquire about disability prior to an offer of employment and must make reasonable accommodations to persons with disabilities.
- **Health Insurance Portability and Accountability Act of 1996** - requires the establishment of national standards for the security and privacy of electronic health care transactions and national identifiers for providers and employers.
- **General Tort Principles** – This includes defamation, slander, libel, intentional infliction of emotional distress, etc. Be mindful that most tort laws have criminal counterparts.

YOU SHOULDN'T BE "FRIENDS" WITH EVERYONE.

On most social networking sites, "accepting" friends or followers is what creates the illusion of confidentiality. For example, many Facebook users set their accounts so that only "Friends" can see their information, and they have to accept the request to be friends. Similarly, most blogs and Twitter accounts have followers. Take time to consider who might read your post, blog or comment. Even if you are careful about who you "accept" as a friend, your friends can pass on your post to their friends, etc., etc. Consider the following scenario:

- *A physician's "friend" on Facebook asks a health-related question, and the physician responds with a form of advisory answer.*
- **Caution:** This seems like just a physician being helpful. He is offering the same type of response one might offer a family friend one runs into at the grocery store. It might be the same question and the same response.
- **Warning:** The physician most likely has created an electronic record of an exchange that could be construed as a physician-patient relationship.

What does this mean: All the risks associated with physician-patient relationships might apply, such as malpractice, patient abandonment and HIPAA.

What to do: Be careful about who may access your social networking accounts. If you wish to take advantage of the benefits of social media, create a personal page, and a secondary page that represents your practice, allowing patients to become fans of only the latter (Berkman, Massachusetts Medical Law Report, Social Networking 101 for Physicians, 2009). Keep your personal social networking pages personal.

.....

EMPLOYEES SHOULD NOT ASSUME EMPLOYER-OWNED EMAIL ACCOUNTS, TELEPHONES, COMPUTERS AND INTERNET ACCESS ARE PRIVATE.

Personal Internet use on the job is a reality. How much will you allow and how will you enforce it? As email communication grows, so does the written record of those conversations. The record rests as a sort of electronic DNA forever. Employers may want to check out what their employees do online. Consider the following scenario:

- *An employee receives a forwarded chain email from a co-worker that is comical, but somewhat inappropriate. As she chuckles a little, she decides another co-worker certainly has the sense of humor to appreciate this, and forwards it on to her. Later, after finding out their employer was monitoring their emails, both employees are fired. (Arace v. PNC Bank, 2005).*

- **Go ahead:** It hardly needs to be stated. In the workplace, email is great. It has become one of the most common vehicles for communication. In 2010, the typical corporate user sends and receives about 110 messages daily. Further, worldwide email traffic was estimated to total 247 billion messages per day in 2009 (The Radicoti Group, Email Statistics Report, 2009-2013 Press Release, 2009). For employees, it has become as ubiquitous as chit-chat around the water cooler.
- **Stop:** Sending an email with an inappropriate joke is much like saying it around the water cooler...while the boss is filling his/her glass.

What does this mean: The general rule is that employers can check email that is written on the company property, or that used the company's email account. So any emails sent at work on company-owned computers, or using a company email account, can be checked by the employer. This usually goes for telephone conversations, voice mails, instant messages and text messages, too.

What to do: Establish guidelines that address privacy expectations. While the majority of courts hold that privacy issues of electronic transmittals at work should be handled on a case-by-case basis (making it difficult to predict the outcomes), courts have provided factors they have considered when determining whether an employee had an expectation of privacy in emails generated at the workplace:

- Whether the company maintains a policy banning personal or objectionable use,
- Whether the company monitors the use of the employee's computer or email,
- Whether third parties have a right of access to the computer or emails, and
- Whether the company notifies its employees, or was the employee aware, of the company's use and monitoring policies (In re Asia Global Crossing, Ltd., 2005).

Businesses should also develop record retention policies and enforce them. Keep only what is required or necessary for business purposes and set time frames for deletion and destruction of routine, unnecessary information, both paper and electronic.

EMPLOYERS SHOULDN'T "GO PHISHING"!

"Phishing" refers to the process of acquiring sensitive information sent electronically, for example, usernames, passwords and social security numbers. Though an employer may not go to this extent, consider the following scenario:

- *Employees at a local restaurant decide to create a personal invite-only blog in which the subscribers could air their work-related gripes about the company, the employers and any general critiques, professional or unprofessional, they might have*

in relation to their employment. One subscriber, a fellow employee of the restaurant, gave her personal password to management, who checked the site and later fired the site creator and another employee. What is right and what is wrong? It depends on the perspective in this one:

- **What is right from employee's perspective:** The Stored Communications Act (and many state versions of it), make it an offense to access stored communications intentionally without authorization to do so. Further, under the National Labor Relations Act, employers are prohibited from disciplining employees who engage in "concerted activity" for the purpose of improving the terms and conditions of employment.
- **What is right from the employer's perspective:** The privacy of the site was fictional. While employees argued it was only accessible by invitees, the creators and writers did not have a reasonable expectation of privacy in the group.

What does this mean: Employers may violate the Stored Communications Act if they access information that requires a password not affiliated with the business. On the other hand, employees should save such colorful writings to formats with a reasonable expectation of privacy, and be careful of who might be reading their posts.

What to do: If you have strict policies on Internet behavior, be explicit and plan to enforce them. However, don't go beyond the public domain in order to regulate employee compliance with those policies (Pietrylo v. Hillstone Restaurant Group, 2009).

WATCH YOUR ENDORSEMENTS.

Many companies spend hundreds of thousands of dollars on marketing each year. Social media platforms serve as less costly marketing vehicles. However, still be wary of people willing to endorse your product or service for free. Consider the following scenario:

- *A physician browses on a rate-your-practice website and finds that a customer has attacked the practice the physician works at, or perhaps even a colleague within that practice, for their atrocious bedside manner and lack of empathy. The physician completely disagrees, and says so in a response to the customer: "You don't know what you're talking about. Dr. Smith is the best family physician I've ever seen."*
- **Go ahead:** Employees are allowed to endorse the company they work for, their co-workers and products or services provided. Further, some of the best advertising can be from your own employees and co-workers.
- **But stop and think:** If the employee's identity is not disclosed in an endorsement, it is deceptive, and may violate the Federal Trade Commission's Guides Concerning the Use of Testimonials and Endorsements ("Guides").

What does this mean: A company can be held liable if their employees are less than honest and a consumer relies on an employee's comments to his/her detriment. The Guides define an endorsement as "any advertising message that consumers are likely to believe reflects the opinions, beliefs, findings or experiences of a party other than the sponsoring advertiser." Further, "any material connection between a person endorsing a product and the company selling the product must be fully disclosed." Material is defined as "a relationship that might materially affect the weight or credibility of the endorsement."

What to do: Make sure all employees understand the risks of deceptive endorsements. Employees should take responsibility for their postings. If statements are in any way related to the company, its products and services or a competitor, the employee should disclose their identity and employment relationship with the company. Further, employees should state whether their views are their own or whether they speak on behalf of the employer, such as, "the views and opinions expressed here are not necessarily those of [Business] and they may not be used for advertising or product endorsement purposes." (Kane, Fichman, Gallagher, and Glaser, Community Relations, Harvard Business Review, 2009.)

.....

IF YOU CAN'T BEAT THEM, JOIN THEM.

Despite the risks, social media can be a helpful tool for your practice. Patients are consumers, and they are using social media for anything from shopping to chatting with relatives in other countries. Consider the following:

- *Hospitals have joined the social media wave, posting videos on YouTube to spread heartwarming patient stories, physicians have used Sermo, a social media site exclusively for doctors, to rally for or against various legislation. The OSMA has also developed several social media tools, including a*

Twitter account, videos on YouTube, a Facebook page as well as a member-protected Community area on our website. Even patients, not subject to HIPAA, can blog freely about specific details of various disorders, ailments, symptoms and treatments. If you aren't keeping up with the trend, you are falling behind.

- **Go ahead:** From a business perspective, it is beneficial to market to a willing audience. Here, that willing audience might consist of hundreds, even millions, of people on the other side of that computer screen. So, engaging in social media can further a business purpose.
- **Caution:** General agency principles apply, and an employer may be liable for the postings of its employees or posts on a site sponsored by the business.

What does this mean: Remember that an employer is liable for the conduct of his employee if the conduct occurred within the scope of his employment. If a business hosts a website in which employees are allowed, and perhaps encouraged to post information, current events, policy changes, etc., the employer could be liable if the employee posts something inappropriate.

What to do: Without question, have a social media policy, and enforce it. Employers should train employees on how, what, and when to write, and then monitor all posts. Employers might limit who may post on behalf of the practice or may require prior approval by a supervisor on some or all posts. Beyond the standard restrictions or prohibitions on social media within the office, if a business wishes to reap the benefits of a business-hosted site, the business should provide a Best Practices guide for employees who might be entrusted with posting information on a company-hosted site. Many company social media policies are posted on company websites for your review. Remember that these policies are very specific to the culture of the company. Make sure your policy has the tone which works with your practice's existing culture.

.....

TOOLS AND RESOURCES

SOCIAL MEDIA RESOURCES AND TOOLS

The OSMA has developed the following templates for use in your practice. Keep in mind that these are provided as examples only.

1. Best Practices
2. Sample Policy: Prohibited Use at Work
3. Sample Policy: Restricted Use at Work

HELPFUL SOCIAL MEDIA WEB RESOURCES

1. **Healthcare Blogger Code of Ethics**
<http://medbloggercode.com/>
2. **Social Media Business Council Resources**
<http://www.socialmedia.org/resources/>
3. **Medicine and Web 2.0**
<http://med20course.wordpress.com/>
Mayo Clinic Center for Social Media
<http://socialmedia.mayoclinic.org/>
4. **Social Media Governance – numerous social media policies posted**
<http://socialmediagovernance.com/policies.php>

BEST PRACTICES

It is easy for social media users to forget that what is posted online is rarely anonymous, it is almost always permanent, and easily searchable and replicable. Add these to the sense of a seemingly invisible audience, and questionable web behavior begins to form and permeate an otherwise satisfactory office social dynamic. When considering a social media policy, here are some suggestions on how to proceed.

1. Have an explicit policy in an employment manual that addresses the following concepts:
 - a. **Accountability and Accuracy.** Posts should be factual. Employees should be responsible for their postings, and should distinguish between their own opinions and that of the employer's. (Kane et al, Community Relations, Harvard Business Review, 2009). If posting on a site that is not employer-hosted or sponsored, employees should not make any reference to their employer or the business. If there is any reference to an employer, an employee should clarify somewhere on the site that "these statements reflect my own opinions and/or beliefs and/or statements and not that of my employer's."
 - b. **Honesty and Transparency.** Identify yourself. Advise employees that any statement must reflect good standards of conduct, judgment, and common sense. If an employee posts a statement that is related to the company or the company's product or service, the employee should disclose their identity and affiliation (Employment Relations Today, 2010).
 - c. **Respect.** Advise employees not to post any derogatory, defamatory, or inflammatory content about others for any reason.
 - d. **Lawfulness.** Train employees so they understand the basic legal and professional framework that governs the company's policies. What is illegal or unethical offline is most likely illegal or unethical online, too. Employees' posts may result in civil liability and other legal consequences. Posts by employees have served as catalysts for claims of defamation, sexual harassment, fraud, misrepresentation, deceptive endorsements and breach of confidentiality and privacy policies.
 - e. **Management.** Notify employees that the company will monitor a broad scope of media, including email and web usage. Conduct in violation of the social media policy is subject to discipline, up to and including termination of employment, and may give rise to legal liability. (Hodgson & Sanders, Federal Regulations Update, Employment Relations Today, 2010)
2. **Monitor Internet Behavior that is conducted on behalf of the company, and have disciplinary actions in place for misuse.** Create and organize supervisors of sites that are hosted by the company. Have those supervisors ensure that employees' writings reflect the concepts above. Establish processes for screening third-party content based on the expected usage and frequency of third party posts. Remove content that is potentially harmful, deceptive, disrespectful and illegal, or content that does not further the purpose of the website and the mission of the practice. If a user violates the terms of the social media policy, implement a disciplinary procedure to address it. Limit employee access to company-hosted sites as well as access to the Internet generally. If an employer ignores damaging material, an employer's lack of action could be perceived as negligent.
3. **Be Collaborative.** Include employers and employees in formulating a written policy. Employees will be more apt to follow a policy if they had a hand in creating it. After gathering information from different perspectives, do a cost/benefit analysis of the various opinions. Ernest Employee would like to be able to visit social networking sites on his lunch break, but Susan Supervisor is concerned about the time it will take to monitor her supervisees. Can they both be happy? If not, which becomes more important?
4. **Contact your liability insurance representative.** First, if it is a practice-hosted site, check and see if your malpractice insurance covers social media. Many insurance policies do not cover emotional distress, which is a fairly common claim in social media suits. If it is a personal site, check your personal insurance coverage. Some umbrella policies cover social media claims. Your insurance company may have their own suggestions, if not requirements, for best practices regarding social media. If your business uses extensive media platforms, consider a media insurance policy.
5. **Add Value.** Provide worthwhile information and perspective. A company's services are best represented by customers and employees, and what your employee shares with others may reflect (positively or negatively) on the company.

SAMPLE POLICY: PROHIBITED USE AT WORK

PURPOSE

The purpose of this policy is to provide [Business] employees with requirements for participation in social media, including [Business]-hosted social media, and non-[Business] social media in which the employee's [Business] affiliation is known, identified or presumed.

[Business] provides to its workforce access to one or more forms of electronic business tools, including email accounts, computers, voice mail, cellular phones, and/or internet use. [Business] encourages the use of these tools to better serve our patients. The tools provided by [Business] to employees are to assist them solely in the performance of their jobs. All users employed by [Business] have the responsibility to use these resources in a professional, ethical and lawful manner. These tools are property of [Business] and may only be used for authorized business purposes.

PROHIBITED USE

Use of [Business]'s computers, telecommunications systems or other electronic software for any of the following activities is prohibited:

1. Sending, receiving, displaying, printing or otherwise disseminating:
 - a. material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating or defamatory;
 - b. confidential, proprietary business information or trade secrets in violation of company policy, employee contract and/or proprietary agreements,
 - c. commercial or personal advertisements, solicitations, promotions, destructive programs and viruses or religious or political material;
 - d. confidential information or Personal Health Information (PHI) in violation of the Health Insurance Portability and Accountability Act (HIPAA) or the Health Information Technology, Economic and Clinical Health Act of 2009 (HITECH), or any other applicable federal, state or local privacy laws; and
 - e. Email or online communications that are solely personal and not in further support of [Business].
2. Using any technology owned and/or operated by [Business] for any personal use, including but not limited to playing online games, visiting chat rooms, shopping online, or engaging in any type of illegal activity, checking personal email or participating in any social media sites;
3. Violating any state, federal or international law governing intellectual property (e.g., copyright, trademark and patent laws) and online activities;
4. Violating any license governing the use of software;
5. Procuring or attempting to procure a password, access a file or retrieve any stored communications without explicit authorization.
6. Endorsing [Business]' products or services or otherwise advertising (including verbal statements, demonstrations or depictions of the name, signature, likeness or other identifying personal characteristics or the name or seal of [Business]) that consumers are likely to believe reflects the opinions, beliefs, findings or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser. This is applicable to personal sites as well.

SOCIAL MEDIA BEST PRACTICES

Personal websites and weblogs have become prevalent methods of self-expression in our culture. [Business] respects the rights of employees to use these mediums during their personal time. The purpose of this policy is to provide requirements for employees of [Business] who participate in social media, in which the employee's [Business] affiliation is known, identified, expected or presumed. Social Media includes but is not limited to, sites that allow an individual or group to share user-generated content, running logs of events and personal insights with online audiences (blogs), online collaboration and publishing systems that are accessible to internal and external audiences (e.g., wikis) and social networking sites (e.g., Facebook, MySpace and Twitter).

- Employees are personally responsible for the content they publish on blogs, wikis, social networking sites or any other form of user-generated media.
- Do not disclose any information that is confidential or proprietary to [Business] or to any third party that has disclosed information to the company. Consult the company's confidentiality policy for guidance about what constitutes confidential information.
- Uphold [Business]' value of respect for the individual and avoid making any defamatory, disrespectful or harassing statements about other employees, members, partners and affiliates of [Business].
- If an employee chooses to identify him or herself as a [Business] employee on a website or weblog, he or she must adhere to the [Business]' Best Practices below:
 - [Business] employees are personally responsible for the content they publish on blogs, wikis, social networks or any other form of user-generated media. Be mindful that what you publish will be public indefinitely.

- Identify yourself. Include your name and when relevant, your role at [Business]. Make it clear that you are speaking for yourself and not on behalf of [Business].
- Abide by all applicable confidentiality laws and policies. Do not disclose any individually identifiable information regarding a member, business affiliate, client or patient of [Business].
- Respect copyright, fair use and financial disclosure laws.
- Company-hosted blogs must focus on subjects related to the organization.
- Employees should seek approval from their supervisor before setting up a [Business]-hosted blog or other social media site or forum.
- Do not disclose any of [Business]' confidential or other proprietary information.
- Be respectful. Do not use ethnic slurs, personal insults, obscenity or engage in any conduct that would not be acceptable in [Business]' workplace.
- Correct mistakes.
- Use citations when appropriate.
- Add value. On a professionally hosted blog, provide worthwhile information and perspective. [Business]' mission is best fulfilled by its employees and members.

WAIVER OF PRIVACY

The electronic business tools are the sole property of [Business]. As such, all passwords, usernames, messages and other communications are the property of [Business]. The federal Electronic Communications Privacy Act creates a right for [Business] to access and disclose all electronic communications, and [Business] reserves such right to monitor, inspect, copy, review and store at any time and without notice any and all usage of the electronic tools, including any and all files, information, software and any other content created, sent, received, downloaded, uploaded, accessed or stored in connection with employee usage and conducted on business-owned property. Employees have no reasonable expectation of privacy with respect to business and/or personal use of business-owned property and employees affirmatively consent to management or supervisory personnel accessing and monitoring any and all material employees create, send, receive, download, upload, access or store. Any failure of [Business] to enforce these rights does not constitute a waiver of such right.

VIOLATIONS AND ENFORCEMENT

Violations of this policy may result in disciplinary action, including possible termination of employment, legal action and criminal liability.

EMPLOYEE ACKNOWLEDGEMENT

I have read, understand and agree to comply with the foregoing policies, rules and conditions governing the use of all property of [Business] and all work and conduct completed on or with the assistance of [Business] property. Further, I agree to abide by the Social Media Best Practices when using social media sites on my personal time and when my affiliation with [Business] regarding those sites is known, identified, expected or presumed.

Name: _____

Signature: _____ Date: _____



SAMPLE POLICY: RESTRICTED USE AT WORK

PURPOSE

The purpose of this policy is to provide [Business] employees with requirements for participation in social media, including [Business]-hosted social media, and non-[Business] social media in which the employee's [Business] affiliation is known, identified, expected or presumed.

[Business] provides to its workforce access to one or more forms of electronic business tools, including email accounts, computers, voice mail, cellular phones and internet use. [Business] encourages the use of these tools to better serve our patients, and to facilitate more efficient and effective distribution of information to co-workers, patients, vendors and other customers for the support and benefit of [Business]. All users of such equipment are responsible for using these resources in a professional, ethical and lawful manner.

To ensure that all employees are responsible and accountable for their usage, the following guidelines and philosophies have been established to assist users when operating or using any electronic business tools.

PROHIBITED USE

USAGE ON COMPANY PROPERTY/[BUSINESS]- HOSTED SOCIAL MEDIA

Use of [Business]'s computers, telecommunications systems, or other electronic software for any of the following activities is prohibited:

1. Sending, receiving, displaying, printing or otherwise disseminating:
 - a. material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating or defamatory;
 - b. confidential, proprietary business information or trade secrets in violation of company policy, employee contract and/or proprietary agreements,
 - c. confidential information or Personal Health Information (PHI) in violation of the Health Insurance Portability and Accountability Act (HIPAA) or the Health Information Technology, Economic and Clinical Health Act of 2009 (HITECH), or any other applicable federal, state or local privacy laws; and
2. Using technology owned and/or operated by [Business] to engage in any type of illegal activity;
3. Violating any state, federal or international law governing intellectual property (e.g., copyright, trademark and patent laws) and online activities;
4. Violating any license governing the use of software;
5. Procuring or attempting to procure a password, access a file or retrieve any stored communications without explicit authorization.

USAGE ON PERSONAL PROPERTY/NON-[BUSINESS] SOCIAL MEDIA OF EMPLOYEE

Use of personal computers, telecommunications systems, social networking or other social media sites and any other electronic software for any of the following activities is prohibited:

1. Sending, receiving, displaying, printing or otherwise disseminating:
 - a. material that is fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating or defamatory against any other person employed by [Business];
 - b. confidential, proprietary business information or trade secrets in violation of company policy, employee contract and/or proprietary agreements,
 - c. confidential information or Personal Health Information (PHI) in violation of the Health Insurance Portability and Accountability Act (HIPAA) or the Health Information Technology, Economic and Clinical Health Act of 2009 (HITECH), or any other applicable federal, state or local privacy laws; and
2. Endorsing [Business]' products or services or otherwise advertising (including verbal statements, demonstrations or depictions of the name, signature, likeness or other identifying personal characteristics or the name or seal of [Business]) that consumers are likely to believe reflects the opinions, beliefs, findings or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser.

BEST PRACTICES

RESTRICTED USE

All electronic equipment, media and services are provided and maintained by [Business], and are primarily for business use and within the scope of an employee's job responsibilities. Limited, occasional or incidental use of electronic equipment or media for personal, non-business purposes is understandable and acceptable, provided such usage is in accordance with the above prohibitions, does not detriment the company, is responsible and ethical, and is not abused. [Business] reserves the right to revoke such privilege at any time.

SOCIAL MEDIA BEST PRACTICES

Personal websites and weblogs have become prevalent methods of self-expression in our culture. [Business] respects the rights of employees to use these mediums during their personal time. The purpose of this policy is to provide requirements for employees of [Business] who participate in social media, including professionally-hosted sites as well as personally-hosted sites in which the employee's [Business] affiliation is known, identified, expected or presumed. Social media includes technology tools and online platforms for integrating and sharing user-generated content, in order to engage others in conversations and/or allow them to participate in or discover new content. Social Media includes but is not limited to, sites that allow an individual or group to share a running log of events and personal insights with online audiences (blogs), online collaboration and publishing systems that are accessible to internal and external audiences (e.g., Wikis) and social networking sites (e.g., Facebook, MySpace and Twitter).

- Employees are personally responsible for the content they publish on blogs, wikis, social networking sites or any other form of user-generated media.
- Do not disclose any information that is confidential or proprietary to [Business] or to any third party that has disclosed information to the company. Consult the company's confidentiality policy for guidance about what constitutes confidential information.
- Uphold [Business]' value of respect for the individual and avoid making any defamatory, disrespectful or harassing statements about other employees, members, partners and affiliates of [Business].
- If an employee chooses to identify him or herself as a [Business] employee on a website or weblog, either professionally hosted or personally hosted, he or she must adhere to the [Business] Best Practices below:
 - [Business] employees are personally responsible for the content they publish on blogs, wikis, social networks or any other form of user-generated media. Be mindful that what you publish will be public indefinitely.
 - Identify yourself. Include your name, and when relevant, your role at [Business]. Make it clear that you are speaking for yourself and not on behalf of [Business].
 - Abide by all applicable confidentiality laws and policies. Do not disclose any individually identifiable information regarding a member, business affiliate, client or patient of [Business].
 - Respect copyright, fair use and financial disclosure laws.
 - Company-hosted blogs must focus on subjects related to the organization.
 - Employees should seek approval from their supervisor before setting up a [Business]-hosted blog or other social media site or forum.
 - Do not disclose any of [Business]' confidential or other proprietary information.
 - Be respectful. Do not use ethnic slurs, personal insults, obscenity or engage in any conduct that would not be acceptable in [Business]' workplace.
 - Correct mistakes, and use citations when appropriate.
 - Add value. Provide worthwhile information and perspective. [Business]' mission is best fulfilled by its employees and members.

WAIVER OF PRIVACY

The electronic business tools are the sole property of [Business]. As such, all passwords, usernames, messages and other communications used in connection with the electronic property of [Business] are the property of [Business]. The federal Electronic Communications Privacy Act creates a right for [Business] to access and disclose all electronic communications, and [Business] reserves such right to monitor, inspect, copy, review and store at any time and without notice any and all usage of the electronic tools, including any and all files, information, software and any other content created, sent, received, downloaded, uploaded, accessed or stored in connection with employee usage and conducted on business-owned property. Employees have no reasonable expectation of privacy with respect to business and/or personal use of business-owned property, and employees affirmatively consent to management or supervisory personnel accessing and monitoring any and all material employees create, send, receive, download, upload, access or store. Any failure of [Business] to enforce these rights does not constitute a waiver of such right.

VIOLATIONS AND ENFORCEMENT

Violations of this policy may result in disciplinary action, including prohibiting an employee from accessing any electronic tools or equipment, possible termination of employment, legal action and criminal liability.

.....

EMPLOYEE ACKNOWLEDGEMENT

I have read, understand and agree to comply with the foregoing policies, rules and conditions governing the use of all property of [Business] and all work and conduct completed on or with the assistance of [Business] property. Further, I agree to abide by the Social Media Best Practices when using social media sites on my personal time and when my affiliation with [Business] regarding those sites is known, identified, expected or presumed.

Name: _____

Signature: _____ Date: _____

