



Solutions in Behavioral Healthcare

Why You Need a Social Media Policy

These days, most organizations have policies on using the internet and cell phones. With higher penalties for HIPAA and HITECH breaches now in place, it is time to add a policy on Social Media.

Social Media includes Facebook, Twitter, LinkedIn, and blogs, to name a few. More are springing up everyday. Here is a quick guide:

[Facebook](#) – by far the most popular of the social media sites – this allows users to text each other directly or en masse, post pictures and other content on their “wall” for invited friends or anyone to see (depends on privacy settings). Users can also join and/or establish networks such as college alumni groups, social workers in Boston, or people interested in Solution Focused Therapy. Facebook can easily be accessed from computers and cell phones with internet access.

[Twitter](#) – A social networking tool that allows users to send messages, known as tweets, to people in their network (called followers). There is a 140 character limit to each tweet. Messages can be sent and received on computers and cell phones.

[LinkedIn](#) – LinkedIn is a business oriented social media site. Users can add contacts and request introductions of other people's contacts (called connections). Uses include posting job information and work related discussion groups.

Blogs – Blogs are usually part of a web site and are used to communicate information, commentaries, videos, and/or pictures. There are blogs about healthcare, news, sports, and maybe even your workplace.

[YouTube](#) – YouTube is a video sharing website, owned by Google.

Social Media can be very useful in healthcare. Information about new treatment groups, health insurance and fund raising are just a few examples. Unfortunately, Social Media can also be extremely risky for a behavioral health organization. A few examples include:

- Staff spending large quantities of time posting on line, chatting, twitting, and not working.
- Without the proper controls in place, Protected Health Information (PHI) can easily be posted to a social media site.
- Proprietary information about your organization can make it out into cyberspace.

In 2008 a group of nurses started posting shift change information on each others Facebook "walls." No patient names were used, but enough information was disclosed to be considered a breach. As in most cases, the intent was not to disclose PHI; but the results can be devastating.

What to do:

- Decide if staff can use social media. If so, what are the proper uses? Who has permission to use them? Will you limit who can "speak" on behalf of your organization?
- Clearly define your policy in writing and educate staff.
- Talk to your IT staff/vendor about blocking certain sites on your network. You can't stop an employee from using their cell phone to post to Facebook, but you can control the use of your internet.

Your policy should include:

- Clear instructions not to post PHI or proprietary information.
- Limits of use and expectations.
- A strong statement that staff are responsible for their personal posts. If identifying themselves as a member of your staff, a disclaimer should be included.

For a list of healthcare social media policies, see: socialmediagovernance.com.

The Mayo clinic guide for employees is comprehensive.

Another good resource is provided by Ed Bennett and can be found at : ebennett.org

For a good overview of privacy issues in Facebook see: <http://www.time.com>

For more information contact:

Jordan Oshlag
Solutions in Behavioral Healthcare
Jordan@Solutionsinbh.com
www.Solutionsinbh.com