www.medscape.com

Hidden Dangers in Your Practice Website

Michael J. Sacopulos, JD | |February 10, 2016

Angry Patients May Attack Your Site

What could be more benign than a basic website? It conveys some information, has some images, and invites the public to "Contact Us." Most medical practice sites are straightforward, noncontroversial, and display the facts. Sure, the website might be as outdated as an avocado-colored appliance, but really, what could go wrong?

Sadly, plenty of things. Take what happened recently to a surgeon in south Texas.

The conversation started awkwardly. "Um, Doctor, there's something you need to know," said the surgeon's patient, who found a website designed to look like the physician's but was nothing of the sort. For example, the "About Us" section contained such statements as, "We recognize this may be a stressful time for you, so we'll do everything possible to make sure we maximize your pain and suffering." Inflammatory fake posts on the site included such comments as "not so sudden death"; "deal with it, junkie"; "kicked to the curb"; and, a perennial favorite, "not my problem." Upon investigation, it was learned that the website had been active for several months.

The surgeon immediately contacted the authorities, who traced the website back to a disgruntled patient. The former patient also happened to be an amateur Web designer. Ultimately, he was arrested for felony online impersonation. However, it's impossible to calculate the actual damage done during the months this impostor website was active.

Although this may seem like an extremely unlikely scenario, there are subtler versions of this behavior that could damage your practice. Recently, an optometrist in the Midwest contacted me to complain that the domain name for his practice—let's call it www.rogersoptical.com—had been purchased by a competitor, who was using it to route traffic to her own website. In other words, when someone typed "Rogers Optical" into a search engine, the rival optometrist's website was the first hit that appeared.

The domain name was legally purchased (my client never laid claim to it), and nothing defamatory about the optometrist appeared on the Web. In fact, nothing at all about him appeared on the Web. The domain was simply being used as a routing tool to direct individuals to a competitor's website.

Sneaky? Devious? Sure, but this scenario isn't unique.

Both the Texas surgeon and the Midwestern optometrist could have avoided their problems by simply buying up some domain names preemptively. Not only do you want to own your practice's domain name, as well as the domain name associated with your personal name, you want to control closely related derivatives. For example, I control not just "Sacopulos.com," but also "SacopulosLawFirm.com" and "SacopulosSucks.com." (Seriously, you can never be too careful.) Domain names are inexpensive to purchase, but can cost you a lot if the wrong person owns them.

A Serious Breach Could Lead to Extortion

If you really want to read something scary, put down that Stephen King novel and google the words "medical website hacked." When I did this recently, I got more than 14 million hits, including such headlines as "Obamacare website hacked," "CareFirst website hacked; 1.1 million affected," and even "Saginaw County Health Department website hacked, health officer says." Your website is a portal to the cyber world. This means not only your patients and prospective patients may visit, but also cyber thieves.

Last year, Harley Medical Group, an aesthetic medicine practice which operates 19 clinics in the United Kingdom, reported that information from approximately 480,000 patients and prospective patients was compromised through

website hacking. Worse, patients' identities were ransomed back to the practice. Unlike most identity thieves, who wish to use the information to obtain credit and goods, these hackers wanted to extort the practice: "Pay up, or we'll release your patients' information."

These types of hacking events are on the rise and should serve as a warning to all of us. I often hear the defeatist attitude, "No matter what I do, my website will not be secure." I agree that it's virtually impossible to guarantee your site will not be hacked. However, that's the medical equivalent of saying, "I'm going to die anyway, so I might as well smoke three packs of cigarettes and eat large hunks of red meat daily."

Think about risk *reduction,* not risk *elimination*. Using good "cyber hygiene" and keeping your systems up to date goes a long way in warding off cyber thieves. Check with the organization hosting your website to see what security recommendations it has.

You May Be Violating Federal Laws

Many doctors are surprised when I tell them that their website must be compliant with the Americans with Disabilities Act (ADA). How so, you ask? For visually impaired individuals, this means the text on a website must be able to convert into audio as the cursor moves across the screen. For individuals who are hearing-impaired, any audio component of the site must be able to be closed-captioned.

In recent years, the National Federation of the Blind (NFB) has brought class-action lawsuits against several retailers, including Target, for website noncompliance with the ADA. In the case of Target, the NFB alleged that the company's website wasn't accessible to blind customers. Ultimately, the class action settled for millions of dollars.

Individuals have also brought these types of lawsuits. A blind mother of three filed a claim against the Seattle public schools alleging that its website software wasn't compatible with a screen reader, an electronic interface that allows blind or visually impaired persons to read text.

The need for websites to be compliant with the ADA isn't new. In fact, all US federal websites have been compliant with the Act for more than a decade.

It's impossible to discuss all the technological options and needs for varieties of websites. I recommend that you speak with your web-hosting service, to confirm that your site's software is compatible with screen-reader software commonly being used today.

Images of Patients Could Be Stolen

"It was both surprising and disturbing," says Seattle-based attorney Greg Wesner, of Lane Powell PC. Wesner recounts the story of representing a prominent West Coast-based facial plastic surgeon whose before-and-after photographs of patients were found on no fewer than 13 other medical practices' websites around the country.

"I don't know whether it was the medical practices or their Web designers who stole my client's images," says Wesner. "What I do know is that it's legally actionable, and we've been successfully going after the practices that display my client's work as though it were their own." (Wesner's client isn't alone; I'm aware of many practices that have faced similar situations.)

Even if you're not concerned that images on your website will be "scraped" and used by others without your permission, you still need to be concerned about this issue. Check to make sure you own the legal rights to every image that appears on your website. Oftentimes, Web designers scour the Internet for nifty images and place them on sites without regard for copyright laws. Big firms such as Getty Images, however, aren't afraid to pursue website owners who use their images without permission.

Although the copyright laws are stacked against you, the good news is that it's relatively inexpensive to secure rights to

use images for your Website. A small amount of effort and expense up front will prevent legal problems and much larger expenses down the line.

Tighten Up Your Disclosures

Just about every website has a "Contact Us" page. This lets a website viewer enter his or her contact information and request a response. Often, these pages have a box where the website visitor may write a message to the website operator.

In the case of medical practices, you need to be very careful when using the "Contact Us" page.

If I call most medical practices at 9 PM on a Friday, I'll get an answering machine. The message will tell me the practice's hours and to dial 911 if I'm having a medical emergency. However, if I access the same practice's website at 9 PM on Friday via the "Contact Us" page, I most likely will not receive the warning to call 911 if I am experiencing a medical emergency. The same warning should appear as a disclosure on your "Contact Us" page.

Other disclosures should be made to prospective users of the "Contact Us" page. If someone types up a long narrative of his or her medical history and sends it to your practice, you may not feel it's appropriate for this person to become a patient of your practice. Therefore, tell users up front that any contact they make with your practice via the website does not create a patient/physician relationship, and does not make the submitter a patient of the practice.

Next, be aware of patient privacy requirements under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. If the communication feature through your website isn't encrypted, and therefore not secure, users should be told this. Something along the lines of "Please know this is not a secure or encrypted means of communicating with our practice" should do the trick.

Many practice websites also contain a "blog" feature. Here, clinicians can provide general medical information and discuss topics that they think may be relevant to their patients. This is a useful feature and a favorite of many patients.

However, you should have a disclosure associated with the blog saying, "This information is *not* meant as medical advice. It is provided solely for education. Our practice would be pleased to discuss your unique circumstances and needs as they relate to these topics." Unfortunately, some people have tried to use medical information from television and blogs as a basis to allege malpractice. Although a blog is not a tremendous area of risk, a simple disclosure may be helpful.

Finally, you may wish to add a "Terms of Use" page to your website, which will touch on a number of different issues, including acceptable use of the site. Examples of "terms of use" for medical practices may be obtained through such organizations as the American Medical Association or some specialty societies.

Protect Yourself—Now!

An ounce of prevention now could save you from losing a pound of flesh later. Now that you've read this article, here's your website "to-do list":

- Buy up domain names that relate to your name and your practice's name. For a few bucks each, this is money well spent.
- Contact whoever helps maintain your website. Ask that person to confirm that security features are in place and are up to date. Next, ask whether your website works with screen readers. If your website uses audio, it should be compatible with closed-captioning.
- Confirm that you have the legal rights to all images appearing on your website. If you don't have the rights to an image, either get the rights or remove the image. No exceptions.

- Finally, make sure your website includes all of the proper disclosures. Your professional association may have templates to get you started.

Like many things in life, your website isn't a problem until it becomes a problem. With a minimal amount of time and expense, you can make sure your website is an asset to your practice and not a liability.

Cite this article: Michael J. Sacopulos. Hidden Dangers in Your Practice Website. *Medscape*. Feb 10, 2016.