Physician Advertising - Proceed With Caution

continued from page 13

1 Education Law §6530(27)

2 General Business Law §649 (Deceptive acts and practices unlawful); §650 (False advertising unlawful)

3 15 U.S.C. §§1-7 (the Sherman Act); 15 USC §§ 41-58 (Federal Trade Commission Act). The Sherman Act outlaws "every contract, combination, or conspiracy in restraint of trade"; the FTC Act outlaws "unfair methods of competition" and "unfair or deceptive acts or practices". The FTC makes available, in 16 CFR Part 255 its Guides Concerning the Use of Endorsements and Testimonials in Advertising, which provides examples of prohibited advertising, including that of medical practitioners, which at this time are prohibited under New York law, but are the subject of a proposed revision to New York's definition of "professional misconduct".

4 Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C. Caution must be taken in writing about specific patients results. Under HIPAA, "there are basically 18 key categories of personal health information that can lead to patient identification and it's easy to inadvertently cross the line" and violate the statute. 7 Dangerous Legal Issues to Avoid in Doctor Advertising, Stewart Gandolf (April 13, 2012 in Advertising, Doctor Marketing, Medical Marketing, Physician Marketing Blog, quoting attorney David Harlow). Consideration must also be given to the HITECH Act (The Health Information Technology for Economic and Clinical Health (HITECH) Act), enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under HIPAA. 42 USC 17921 et seq.

5 www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/antitrust-laws - The penalties for violating the Sherman Act can be severe. Although most enforcement actions are civil, the Sherman Act is also ab criminal law, and individuals and businesses that violate it may be prosecuted by the Department of Justice. Criminal prosecutions are typically limited to intentional and clear violations such as when competitors fix prices or rig bids. HIPAA violations may also be the subject of a criminal prosecution. 42 U.S.C. § 1320d-6(b).

6 Education Law §6530; Public Health Law §230(1); see, e.g., Citroenbaum v NYS Dep't of Health, 303 AD2d 855 (3d Dept. 2003); and Gant v Novello, 302 AD2d 690 (3d Dept. 2003) (both cases involving physicians having falsely advertised and fraudulently practiced based on misrepresentations of their credentials); see also NYS DOH State Board For Professional Medical Conduct Statement of Charges (available on DOH website) - Matter of Severinsky, wherein the practitioner "knowingly inappropriately advertised himself on a web page on the Internet and in related email correspondence as in independent practicing psychiatrist" at a time when he was in his residency.

7 421 U.S. 773 (1975)

8 www.ama-assn.org/ama/pub/physician-resources/medical-ethics/8 code-medical-ethics/opinion502. Physicians are encouraged to review the guidelines and ethical opinions promulgated by the AMA and the Federation of State Medical Boards ("FSMB") regarding advertising and the use of electronic media.

9 Education Law §6530 (b)

10 Education Law §6530(c)

11 Education Law §6530(d)

12 7 Dangerous Legal Issues to Avoid in Doctor Advertising, Stewart Gandolf in his Advertising, Doctor Marketing, Medical Marketing, Physician Marketing Blog of April 13, 2012.

13 There have been recent efforts to include that requirement, in proposed New York Senate Bill S5493, which would enact the "Health Care Professional Transparency Act". The New York Coalition of Speciality Care Physicians has issued a Memorandum in Support of the bill, stating that "[h]ealth care professionals representing themselves as board-certified would need to disclose the full name of the certifying board. Ambiguous nomenclature, related advertisements and marketing, and the myriad of individuals one encounters at each point of service all contribute to patient confusion. Patient autonomy and decision-making are jeopardized by uncertainty and misunderstanding in the health care patient-provider relationship."

14 Small v Lorillard Tobacco Co., 94 NY2d 43, 55 (1999)

15 Karlin v IVF Am., 93 NY2d 282, 290-291 (1999); see also Johnson v Body Solutions of Commack, LLC, 19 Misc3d 1131(A), (Dt. Ct of New York, Suffolk Co., 2008).

16 Oswego Laborers' Local 214 Pension Fund v Marine Midland Bank, N.A., 85 NY2d 20, 25 (1995)

"2014: The Year of the Breach?"... you 'aint seen nothing yet'

Bill Palisano
President of Lincoln Archives

I didn't make that title up, I've read that statement several times in various information security reports and breach reporting publications that I follow. Google it, you'll see. We're all familiar with the Sony, the Target, the Home Depot, the 'Russian', the (fill in the blank)...Breach. (Even though Target happened in 2013, we started seeing the fallout in 2014). Hate to say it, but are we becoming desensitized about breaches? I hope not. Many of the breaches you've read about resulted in your credit card or debit accounts being compromised (aka: stolen). These types of thefts can be serious or merely a nuisance.

But there are much more serious type's of breaches which results in potentially life changing and even life ending events. We're talking theft of social security numbers and medical ID's. Welcome to 2015; here's a new, major one: The "Massive Anthem Data Breach." Hot off the presses.

Per the Pittsburgh Post-Gazette (2/25/15): "The (Anthem) breach, disclosed at the beginning of (February), resulted in the theft of personal information for 78.8 million people, including current customers and employees, and former customers and employees dating back a decade — plus as many as 18.8 million customers (or as few as 8.8 million) from affiliated Blue Cross Blue Shield health plans. Anthem, the nation's second-largest health insurer, says hackers may have gained access to customers' names, addresses, medical IDs, Social Security numbers, birthdays, and even job and income data."

Now, why are these types of breaches/thefts comparatively worse? It's because once a thief has your social security number, he or she can effectively 'become you'. He/she can take out credit in your name, buy cars, houses, toys, you name it. This is known as 'the credit you don't know about'. After sixty days, if undisputed – you own the debt. You can dispute it, but you own it now. It's up to you to prove 'it wasn't you'. This is not a 'nuisance'. In 2013, stolen social security numbers were selling on the black market for $3.00. Per "Finding a Cure for Medical Identity Theft" (published by CSID, October 2014, researched by Research Now), in 2014 that number dropped to $1.00! Sickening, isn't it?

Breaches where social security numbers AND medical ID numbers are both compromised lead to the fastest growing form of identity theft: Medical Identity Theft. Medical Identity Theft includes fraudulent use of another's identity to purchase medical goods/services, prescription drugs, and defrauding medical insurance payers including Medicare/Medicaid.

Per Rick Kam, president and cofounder of ID Experts: "Essentially, criminals have come to understand that using your medical credentials—your name, Social Security Number and health insurance numbers—to order goods and services that are never delivered and to bill organizations like Medicare and Medicaid, those activities are more profitable than drugs, prostitution, and other crimes they may pursue. For this reason, medical identities are 20 to 50 times more valuable to criminals than financial identities."

One of the greatest dangers of someone else 'becoming you' is the risk that they change your medical profile. There are many documented cases where people have died because medical profiles were changed including blood type, allergies, insulin use, medications, etc. If you are unconscious, you cannot say 'I am/am not a diabetic' 'I do/do not use insulin', 'I'm allergic to...' etc. This is a major concern.

Per the Ponemon Institute's: "5th Annual Study on Medical Identity Theft" (published February 2015, sponsored by MIFA – Medical Identity Fraud Alliance), in 2014, Medical Identity Theft increased by 21.7 %., over 2013! That is on top of a 19% increase in 2013 over 2012. The numbers are staggering. Do the math: that's a 44.8% increase in 2 years!

So what does all this mean to you? Per Ponemon's 2015 study, if you're a victim of Medical Identity Theft:

1. Only about 10% of you will achieve a satisfactory conclusion of the incident.
2. You will spend a lot of your time trying to resolve (more than 200 hours).
3. You will spend a lot of your money trying to resolve (65% of victims spent more than $13,500).
4. Your reputation may be negatively impacted (45% of victims experienced embarrassment due to disclosure of sensitive health conditions).
5. You will probably consider changing the

continued from page 15

healthcare provider responsible for the breach (48% of victims in study reported this).

So what can you do to reduce your risk of being a victim? First and foremost, review any medical invoices mailed to you. If something doesn't make sense – investigate it right away. Periodically request (if necessary) and review any EOB (Explanation of Benefits) provided by your medical insurance provider, Medicaid or Medicare. If a collection letter for medical services is received and makes no sense, do NOT dispose of it, assuming it's a mistake. Investigate it, immediately. Protect your medical credentials – even from family (sadly, per the Study, 24% of victims had family members who stole and used theirs).

You may consider an Identity Theft Protection plan. There are many out there – some better than others. Honestly, like medical insurance, I feel that these types of plans/coverages will one day be pretty much widely used and/or necessary. Like medical insurance once was, nowadays we all have to have some form of it. So, if you consider an Identity Theft Protection plan, know exactly what the provider offers, and how much they will do for you versus what you have to do for yourself. There is a difference between identity theft 'resolution' and identity theft 'restoration'. Read the small print on their agreements.

Simply, be informed about Identity Theft and be prepared. With the Anthem Breach alone, we've started 2015 with possibly 79 million personal identities being compromised. The bad guys know there is money to be made. The good guys are trying to protect you. Do not be oblivious and do not become desensitized. Be proactive and vigilant, not a victim.

The Erie County Medical Society
Cordially invites you to attend the

2015 Annual Meeting and Installation of Officers
Wednesday, May 6, 2015

Hyatt Regency Buffalo
2 Fountain Plaza, Buffalo, New York

5:45 p.m. – Cocktail Reception followed by Meeting and Dinner

Guest Speaker
Carl Paladino, CEO of Ellicott Development Company

Presentation of Awards

NO CHARGE FOR MEMBERS - $100 per person/Spouse & Guests

2015-2016 County Society Officers will be installed

Please RSVP no later than Friday, April 24, 2015 with payment included.
PLEASE PRINT ALL INFORMATION LEGIBLY

Physician Member Attending

Phone_____ Fax_____

Email _____

_____#of Guest(s) Attending at $100 each _____ Total Amount Enclosed

Name of Guest(s) (add additional sheets if necessary)

_____

_____

Return to: Erie County Medical Society ◊ 2015 Annual Meeting /Dinner ◊ 1317 Harlem Road ◊ Buffalo, NY 14206

No Show Policy: Members & Guest(s) will be charged $100 if cancellations are not received and confirmed by Friday, April 24, 2015