# "Doctor, turn on the TV. We made the news. Uh-oh, this isn't good!"

*By:* Bill Palisano, Lincoln Archives

Okay, you've read the riot act to your staff, something like: "No patient information goes into the trash, into the recycling bin, or goes home. All paper files, films, etc., gets shredded. Any backup tapes/drives etc., are encrypted before they leave these walls. Etc., etc., etc." So you felt pretty good. You told your staff what to do, and as we all know:

1. Every member of our staffs does everything, exactly like we want them to, when they're supposed to, every time.
2. We have plenty of staff, who never get behind and don't feel they need to cut corners or take short cuts.
3. Each staff member understands every task he/she is supposed to perform, each has the memory of an elephant, and never forgets every rule, process and timetable. They are so good that even if we don't tell them exactly what to do, they are so smart, they'll figure it out, and do it exactly right.

So, you've given them the directions, and now they'll perform perfectly, every time. You're covered, right? Besides, big breaches used to happen but incidences have significantly been reduced as everybody is smarter and more security conscious, right? HHS/OCR isn't really serious about enforcing HIPAA, and don't police it anyways, right? If we were to have a breach, we'd have plenty of time to figure out how to handle it, and we'd probably just get a slap on the wrist (the first time), right?

Are you asking yourself "Is he serious?" Of course, you are. And of course, I'm not. Ignorance may be bliss, but it'll sure be expensive. A couple recent events you might find interesting:

**"Medical Identity Theft Increasing** / *NPR Marketplace / June 21, 2011*

NPR's "Marketplace" recently covered the increase in medical identity theft and, focusing on the devastating effects on its victims. As the article demonstrates, not only does medical ID thefts have a financial component, it also changes the person's medical history; putting them at risk of improper care in the future."

**"Contractor Appointed to be HIPAA Cop** / *Government Health IT / July 6, 2011*

On June 10, 2011, the Department of Health and Human Services (HHS) awarded to KPMG a $9.2 million contract to create an audit protocol and to then audit covered entities' and business associates' compliance with the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)."

**"Delayed Breach Notification Leads to Fine** / *Indiana Attorney General / July 5, 2011*

A release by the Indiana Attorney General Greg Zoeller reports that an Indiana-based insurance company will pay a $100,000 fine and take other steps for waiting months to notify authorities of a data breach. According to the release, Wellpoint, the Indianapolis-based parent of Anthem Blue Cross and Blue Shield, has agreed to pay the fine; provide up to two years of credit monitoring and identity theft protection to affected customers, and reimburse up to $50,000 for breach-related losses. HIPAA now requires all Covered Entities and Business Associates (vendors) to report data breaches to authorities, affected consumers and, in some cases, the media."

**"Big Breaches Build Momentum for Federal Data Protection Law** / *Insurance Networking News / June 22, 2011*

According to a report in the Insurance Networking News, recent data breaches are building momentum for a national standard for breach notification. The report states that during a recent Senate Banking Committee meeting, financial services representatives spoke in support of an Obama Administration plan to "combine a patchwork of 47 state laws on the issue into a federal standard." In addition, Senate Banking Committee Chairman Tom Johnson is reported to have said, "Breaches are disruptive and raise the potential for financial fraud, identity theft and, potentially, severe threats to our national economic security."

So, people are still making mistakes. Identities are still being compromised and/or stolen. Businesses are still paying dearly. And our government is just starting to ramp up. On top of that, there's still that potential sick feeling that you could see your name in the news. "Bad day at the office," "Cheer up son," "have a Lifesaver" is not going to cut it, here. Nope, not by a long shot.

How do you protect your practice from itself? Elementary, my dear Watson. It starts out a bit complicated, but then gets easier. I'm going to simplify/shorten this as I don't have unlimited real estate in this magazine (also, my 13 year old daughter/editor is beginning to yawn). You start at the start.

First, you have to come up with YOUR security policy. One size does not fit all. You have to identify your risks. You have to have policies and procedures in place to mitigate those risks as much as possible. There has to be a chain of command, and someone ultimately charged with enforcing and auditing within your practice (or department). There also has to be a process in place to address what to do if there is a breach, or a reasonable suspicion that there is or could be a breach, including who to notify within the organization, and a timetable as to when things should happen.

Next, you have to have a process in

*Continued on page 15*

## How to Slash Accounts Receivable

*Continued from page 11*

what he might do with it in the kitchen. They regularly shoot credit card numbers into a black hole in the Internet. So why should they object to doing the same thing with their medical bills?

Some will object initially. But when we explain that we're doing nothing different than a hotel does at each check-in, and that it will work to their advantage as well by decreasing the bills they will receive and the checks they must write, most come around.

One medical practice incorporated this strategy as mandatory. Why? Because in only a year their accounts receivable totals dropped by nearly 50%. They are now the lowest they have ever been, in all categories, in 24 years of practice.

It's time for physicians to do more of what they do best--treat patients--and leave the business of extending credit to those who do that best.

Just as people need blood circulating through their veins, so do medical practices need revenue flowing through their bank accounts. Transworld Systems has helped many clients keep the life blood of their medical practice flowing

Transworld Systems specializes in complete billing and follow up services for a wide variety of medical practices. Their expertise enables them to convert accounts receivable into cash. Our foundation is built upon experience, credibility, technology and a proven track record.

- Experience: Our experienced staff monitors industry regulations. In addition, we constantly review our clients' accounts - a practice that enables us to identify opportunities for improvement.
- Credibility: In addition to their status as a preferred vendor of the Erie County Medical Society, Transworld has a status of "preferred vendor" or "endorsed vendor" with 10 county medical societies throughout New York State. In addition to that, their program is sponsored by the American Medical Association (AMA), they have a "Peer Reviewed" designation by the Healthcare Financial Management Association (HFMA), and they are the only collections company to be an AdminiServe partner of the Medical Group Management Association (MGMA).
- Technology: Transworld's online client portal allows for our clients to immediately know the status of any patient account that has been submitted. In addition to that, they have partnered with many practice management companies to create an interface to seamlessly manage their accounts receivables.
- Proven Track Record: With more than 25,000 medical clients nationally, their program has been tested and proven for more than 40 years. The organizations listed above have audited their results and concluded that Transworld Systems provides an industry best practice for converting accounts receivable into cash.

*This article was written by Tom Venturini with Transworld Systems. Tom has been a consultant with Transworld Systems for over 8 years and works with hundreds of different clients. Tom can be reached at 315-445-1375, or by email at Thomas.venturini@transworldsystems.com*

## Doctor, turn on the TV.

*Continued from page 6*

place to educate and update training of your staff on following YOUR security policy. Do not forget to educate NEW employees, from their very start.

Lastly, it is CRITICAL that EVERY EMPLOYEE acknowledges that he/she understands the policy, agrees to follow the policy, and that (here is the most critical term) he/she acknowledges, understands and agrees that his/her ongoing compliance is a condition of his/her employment.

"So what Bill, another process, plan, procedure, blah, blah, blah, same as everything else" you say? Not by a long shot. By making each employee's employment conditional to complying, you are doing two things:

1. Making that employee think twice before he/she breaks the rules, possibly costing his/her job (self policing).
2. Reducing potential liability for the practice and shifting some of the responsibility, risk, and potential penalty from the practice to the individual.

Where is that assumption coming from, you ask? HIPAA regulators have written that when employees are appropriately trained on proper disposal, healthcare providers will not be held fully responsible for disposal violations. At the same time, HIPAA regulators have stated that failure to provide such training will result in the highest level of mandatory fines. And that difference could be the difference of being fined: $1000 minimum per violation (Reasonable Cause) vs. $50,000 minimum per violation (Willful Neglect)*.

And that's reason your practice should have a formal program in place. HHS/HIPAA's Compliance Enforcement 'cold and flu season' is coming. Time to take an "ounce of prevention."

*Source: http://www.ama-assn.org/ama/pub/physician-reources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page