



Welcome to 2015, y'all. Read the following to see why this year may be the year of the Medical Wild West.

How EMR shares data with....everyone

Computers in medical offices are everywhere. From the simplest note-taking to the intricacies of reconstructing images on MRIs, healthcare is becoming digitized. The most intrusive manifestation of this is the directive that all healthcare professionals use electronic health records or face ever increasing financial penalties. The public and the medical community are told the tremendous upside of universal records -- mainly that they are the panacea to every medical woe from health care costs to medical errors. Rarely are patients or doctors told the massive downside of this same system.

Physicians have been incentivized to bring electronic medical records into each and every office. Under the government program 75% of eligible doctors and 92% of hospitals have received "incentive payments" (a very fancy set of words meaning bribes). However, hacking and the unauthorized disclosure of private information are making headlines almost every day. What does this mean for our most private information? If you are looking for comfort, stop reading now!

Are you still with me? OK, here we go! Let's do a little dabbling and ask which government bureaucracies have access to our health care information. Thirty five federal departments and agencies plan to share your information to "improve health care". Review the list below and you will see such entities as the Departments of Agriculture and Defense on the list. Let's not forget NASA and the office of Civil Rights. All will have access to EHRs, as well as other electronic medical information, such as mobile and tele-health technologies, medical devices, sensors and remote monitoring devices. Do you know how many thousands upon thousands of people will have access to your data? All it takes is one hacker or one dissatisfied worker and your information is open for all to see. Just today, as of

this writing, the fairly unsophisticated ISIS hackers have gotten into the Pentagon database and published data from US CentCom. If you believe your data is more secure than the Pentagon, maybe you should stop reading right here. If you would rather continue to live in blissful ignorance, do not continue!

Participating Federal Departments and Agencies

- Administration for Children & Families (ACF)
- Administration for Community Living (ACL)
- Agency for Healthcare Research and Quality (AHRQ)
- Centers for Disease Control and Prevention (CDC)
- Centers for Medicare & Medicaid Services (CMS)
- Department of Agriculture (USDA)
- Department of Defense (DOD)
- Department of Education (DOE)
- Department of Justice (DOJ) and Bureau of Prisons (BOP)
- Department of Labor (DOL)
- Department of Veterans Affairs (VA)
- Federal Communications Commission (FCC)
- Federal Health Architecture (FHA)
- Federal Trade Commission (FTC)
- Food and Drug Administration (FDA)
- Health Resources and Services Administration (HRSA)
- HHS Assistant Secretary for Financial Resources (ASFR)
- HHS Assistant Secretary for Health (OASH)
- HHS Assistant Secretary for Legislation (ASL)
- HHS Assistant Secretary for Planning and Evaluation (ASPE)
- HHS Assistant Secretary for Preparedness and Response (ASPR)
- HHS Office of the National Coordinator for Health Information Technology (ONC)
- HHS Office for Civil Rights (OCR)
- HHS Office of the Chief Information Officer (OCIO)
- HHS Office of the Chief Technology Officer (CTO)
- HHS Office of the General Counsel (OGC)
- HHS Office of Minority Health (OMH)
- HHS Office of the Secretary (OS)
- Indian Health Service (IHS)
- National Aeronautics and Space Administration (NASA)
- National Institutes of Health (NIH)
- National Institute of Standards and Technology (NIST)
- National Science Foundation (NSF)
- Networking and Information Technology Research and Development (NITRD)
- Office of Personnel Management (OPM)
- Social Security Administration (SSA)
- Substance Abuse and Mental Health Services Administration (SAMHSA)

Things about the Sony Hack You Don't Know

If this is not enough to scare you, did you know that the hackers of Sony's computer systems (whether North Koreans or disgruntled employees), were able to pull out detailed and identifiable healthcare information on more than three dozen employees, spouses and their children? Remember, any communication within your email may disclose key information. Here is what was disclosed for one Sony employee:

One memo by a human resources executive, addressed to the company's benefits committee, disclosed details on an employee's child with special needs, including the diagnosis and the type of treatment the child was receiving.

What if that was you, what if that was your child? If that was not enough, another memo that was hijacked disclosed on a spreadsheet the names, birthdates and medical costs for 34 Sony employees who had particularly high costs. The conditions included cancer, alcoholic cirrhosis, premature births and kidney failure.

Remember once this information goes on the internet, it is there forever. Once it is there, anyone can look at your personal information at any time, under any circumstances.

One e-mail between Sony's insurer, Aetna Inc., and its human resources department over a denied claim contains the name of an employee and the type of surgery the worker's spouse had. Another between health insurer Anthem Inc. and Sony's human resources department includes the name of an employee and an unresolved claim for speech therapy sessions. In the memo discussing denied claims for the employee's special-needs child, Sony's human resources department went into great detail on the type of treatment the child was getting, how the child was faring, the location of the facility and conversations the insurer had with the child's care providers.

If you think this Orwellian, it is. Privacy, one of our most cherished values, is rapidly being lost in the name of technological advances. This is not to say we should all become luddites in our outlook. But it should cause us to pause and reassess the situation. It should cause us to ask questions about security and privacy instead of rushing into digital nirvana. As data is entered into EHR systems, one must realize that, in all likelihood, it cannot be protected from a resolute hacker or institution who is willing to spend the time and effort to garner your information.

According to an MIT review, hackers stole a record number of medical records in 2014, but 2015 is supposed to be much worse. A US privacy think tank reported that fully 40% of health-care organizations reported being attacked by malware designed to steal data. The Privacy Rights Clearinghouse reported that 4 million MORE records were stolen in 2014 than in any other year.

There are several take home lessons. These are the ones I keep reminding myself about:

1. Be very careful what you enter into medical records.

2. Realize that the priority of most medical records is not security but complying with governmental medical regulations.
3. Be aware that you may not realize that your records have been compromised.
4. A final thought that is only my opinion and not condoned by “the government”. I purposely do not put some data into my records. If this means that I get penalized for not completing some meaningful use, so be it. We are all free individuals and must draw our own lines in the sand.

Remember, hacking medical records is far more lucrative than simple credit card hacking. With medical record hacking comes not only financial information, but massive amounts of demographic information, including addresses, phone numbers, next of kin, social security numbers, insurance numbers, health information and so much more. In fact, with this information the hacker can construct an entire persona of you without you even knowing it. This is not comforting. Nor is the fact that, at this time, the hackers appear to have the upper hand against internet security programs.

Your Doctor Can't Be Found

The NY Times is a large proponent of the Affordable Care Act. That is why articles that discuss the negatives, though few and far between are so informative. As you know, Obamacare has shifted large number of patients into Medicaid. But the NY Times published a report by the Inspector General that has found that one half of doctors listed as serving Medicaid patients are unavailable to patients. More than 1/3 weren't even at the address listed. Many of the providers had left the location months to years before their listing. Once a physician was found over one quarter had wait times over one month. Obviously, someone's idea of a provider network is a little different than mine and what was laid out in the run up to the enactment of the healthcare law.

There Goes Corporate Wellness

One of the big pluses of Obamacare was supposed to be corporate wellness programs. Well check that puppy off the list of benefits. As part of the program, many of enrollees could reduce their monthly tab by participating in monthly screenings, weight loss programs and other modalities. Enter the EEOC (Equal Employment Opportunity Commission) who is arguing that making employees have medical testing is in violation of the American Disabilities Act.

Don't you just love it when two bloated government bureaucracies fight each other in a cage-match? They should sell tickets.

Oh, but the story gets even funnier, because the newest literature does not show that corporate wellness programs are beneficial.

“Despite employers’ enthusiasm for wellness programs, ‘there’s no good research that shows these programs actually improve health outcomes or lower employer costs,’ says JoAnn Volk, a senior research fellow at Georgetown University’s Center on Health Insurance Reforms.”

Really, you simply cannot make this stuff up!

Get Ready For Penalties

Did you know that as of now, January 2015, 257,000 physicians will face a 1% cut in our Medicare reimbursements for not meeting meaningful use (MU)? Another 28,000 will face an additional 2% cut for not meeting e-prescribing standards. Not impressed, okay how about this...as of November, 2014 only 2% of us had completed MU2, meaning 98% of us are up for additional penalties. So get your mouse fingers ready and start checking useless boxes that in no way improve patient care. If you think the information you provide is secure, please re-read the first article. Apply, rinse and repeat as often as necessary until you finally grasp the situation.

IMPORTANT TAX INFORMATION:

If you obtained insurance through the exchange, you have new tax forms to fill out... Form 1095-A, the Health Insurance Marketplace Statement. What on earth is a “1095-A” you ask? Well here is the answer:

Form 1095-A reports the total monthly health insurance premiums paid to the insurance company you selected through the Marketplace. It also details the advance payments of the premium tax credit that were paid directly to your insurance company.

If you obtained insurance through the exchange, you need to watch out for this form arriving on your doorstep. It will arrive by snail mail. The form is to be sent by January 31, and you can't file your regular taxes without it. If you do not receive your 1095-A, or if it is lost or is wrong, you need to contact the

Marketplace directly. That's right, the same Marketplace that was a giant failure last year. The IRS is not going to be able to answer questions about the information on Form 1095-A or about missing or lost forms. To make things, "ahhhhhh..... easier", the IRS has just published a 21 page pamphlet on how the Affordable Care Act affects taxes. You can get it by asking for IRS Publication 5187. Put it in your library alongside The Complete Works of Shakespeare, Boccaccio's Decameron and Tolstoy's War and Peace.

What the Future Holds

It is my belief that 2015 will be the equivalent of the Wild West in medicine. Boomtowns or boom practices will rise and fall, judicial decisions will turn things inside out, shoot outs between government agencies and political parties will cause doctors and patients to run for cover. Too many regulations will end up meaning no one has any idea what they need to do to comply. Massive change is in the wind. PPD is here to help you survive. Please think about re-upping your membership. Give me a call at (310) 859-9258; we have a whole slew of price saving features that may very well turn you into a survivor.
