Opinion

Orlando Sentinel
Nancy A. Meyer Publisher and CEO
Paul Owens Opinions Editor

SOMETHING ON YOUR MIND?
Ideal letters to the editor are brief and to the point. Letters may be edited for clarity or length. Submissions require the writer's name, address and day and evening phone numbers.

Mail: 633 N. Orange Ave., Orlando, FL 32801
E-mail: insight@orlandosentinel.com
Web: OrlandoSentinel.com/letters

THE FRONT BURNER

Digital health records: pain and gain

Access to information critical despite trade offs

By Nick van Terheyden | Guest columnist

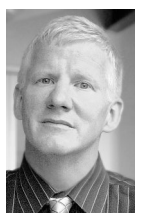
A recent study published in Forbes shows that 80 percent of patients are concerned about the safety of their health information.

And they should be.

Our data will never be 100 percent secure. This is a reality we all face as denizens of the 21st century. We live in a world where everything from our banking transactions to the diagnostic reports mechanics run on our cars rely on digital capabilities that have been designed to provide real-time results in a user-friendly way. Potential data breaches are the trade-off we make for that instant access; in health care, access to information is critical to providing the best patient care.

The repercussions of a health data breach are not the same as, say, a hacking into your Instagram account. While both are undesirable, they are not of the same gravity. Health data has the potential to impact everything — from our health insurance premiums and life insurance rates to how we are treated in the workplace. However, all patient data are not the same, which means that security measures and access should not necessarily be uniform for all information types or roles.

Consider a nurse who needs to access a patient's phone number to inform him of his weekly Coumadin levels. This contact information could be most likely found via a quick Internet search using an online white or yellow pages, so should not require elaborate security measures. Conversely, a physician who is electronically ordering oxycodone for her patient who has just undergone spinal surgery should indeed be required to authenticate her identity and that of the patient through a more rigorous security process.



As health-care professionals, we are not just entrusted by our patients with their physical health, but with their personal health data.

Since security measures are not a one-size-fits-all regimen, the challenge quickly becomes how do we strike a balance, developing and implementing secure processes that do not simultaneously create obstacles for health-care teams?

At the recent Mass TLC Health Summit in Boston, Adam Landman, chief medical information officer of Health Information Innovation and Integration at Brigham & Women's Hospital, spoke on the issue of health IT security. He rightly pointed out that because of the nature of personal health information, health-care organizations can't just bolt any security program onto their existing systems. In fact, security consists of more than just software and consistent data tracking and auditing. There need to be processes and check points in place to ensure that the system, and its many users, both clinicians and patients, consistently meet expectations in upholding these important measures.

The good thing is that the health-care industry has many of these measures already in place. Physicians have national provider identifiers, rotating passwords, phone locks and encryption systems on their devices — you get the picture. What is essential is that health-care organizations continue to monitor, update policies that include rules for "bring your own device" and ensure their servers are secure. Additionally, they must be vigilant that when they integrate other medical practices and facilities into their organization, that they extend these measures to incorporate new employees, new sites and locations and their various technologies.

While we all strive for 100 percent security in every industry, given the ubiquitous and complex systems that continue to expand into every aspect of our modern lives, it is impossible to predict all conceivable outcomes; therefore, failure of some form is unavoidable. However, by building security into the core of our systems and ensuring it is present in every aspect of our interactions with our patients and their data, we can design and test systems and solutions that, should they fail, do so securely. As health-care professionals, we are not just entrusted by our patients with their physical health, but with their personal health data as well. We need to treat both with the same level of respect and importance.

Nick van Terheyden, MD, is chief medical information officer for Nuance Communications.

Today's moderator

DARRYL E. OWENS
Editorial Writer

Five years ago, America seemed headed the way of Star Trek's "Bones" McCoy. The 2009 economic stimulus poured nearly $26 billion in digitizing medical records.

And doctors were eager to beam up their patients' records into virtual storage.

More than 2,200 Central Florida doctors adopted digital record-keeping aided by the University of Central Florida College of Medicine's Regional Extension Center.

The potential was clear. Electronic health records promised a vehicle for doctors to share easily and quickly patient data, significantly reduce prescription drug errors, and allow patients convenient access to their records.

In many cases, it has worked as advertised. Yet, as a recent Pittsburgh Post-Gazette article noted, there have been bugs that have proven tough to inoculate against and have resulted in a rise in the number of complaints about the systems to the FDA's adverse-event database.

Beyond complaints from the practitioners working with the system, there are lingering privacy concerns and worries about identify theft.

Both of today's columnists acknowledge transitioning to computerized records is both a boon and burden; one sounds a louder note on security concerns, while the other argues the rewards of universal access are worth the risks.

By the numbers

■ **48 minutes:** Free time per clinic day that physicians reported losing due to electronic medical records, according to a study published in November in the journal JAMA Internal Medicine.

■ **$24 billion**: The amount that the U.S. Centers for Medicare and Medicaid Services has handed out to hospitals and doctors looking to overhaul their digital records systems and ditch paper record keeping.

Fast-paced society needs medical data to keep up

By Rob Faix | Guest columnist

Electronic health record systems are a boon and a security risk. Today's electronic health systems with advanced monitoring capabilities like the ability to detect potentially adverse drug interactions as medications are being prescribed to a patient are critical. No one would question whether this information is a significant benefit.

The electronic health record systems of today are far superior when considered against the alternative, a paper record. The world we live in continues to go digital whether it be our pictures, our videos, or our letters to grandma. It is only natural that our handwritten medical records — stored in folders in the doctor's office or in our hometown hospital records room — follow the same course. The reality is that the world we live in today is already connected and some might argue that health care as an industry is, in reality, playing catch-up to other industries such as retail and finance.

While some of us may still use paper checks, all of our financial information is housed electronically with our banks and the vast majority of us not only accept, but embrace it. We can now pay our bills online, receive alerts should the balance in our checking account be at risk for overdraft, and even view an electronic version of the check we recently wrote. When we're checking out at our favorite big-box retail store, we can receive an alert of an instant savings. Why? Because everything about our purchases is being logged and can be tied back to us as individual shoppers.

Access comes at a price. As medical information is digitized, it becomes accessible and must be secured; and security is a cat and mouse game.

Further fueling interest in implementing and connecting advanced electronic health record systems is the fact that we are a society on the move, more so now than ever in our nation's history. As I'm writing this article today, I'm in Orlando, 700 miles from my home on a business trip, along with the tens of thousands of people from around the world who visit this city daily. It is imperative that today's electronic health-record systems are universally connected so they can share potentially lifesaving medical information from any health-care system. That is the long-term vision for the health-care industry and would provide tremendous value to us as patients. We should want the doctor providing care to have all the potential medical history about us and our families as they begin to make decisions on how to best to treat the situation.

Access to information does come at a price. As medical information is digitized, it becomes accessible and must be secured. Plenty of technologies exist to secure medical information, but another hard reality of the world we live in is that security is a cat and mouse game. There are people around the world who attempt to hack into hospital systems every second of every day, and for the most part, they are unsuccessful due to preventative technologies in place. Regulations are in place that require hospitals with electronic health records to attest to the fact that they have performed annual security audits to ensure proper security measures are in place to protect all medical records.

However, nothing is a guarantee. If a breach of medical information should occur, hospital systems are required, by law, to notify you once the breach is confirmed and make resources available to further discuss the matter with you directly. Breaches do and will continue to occur. Not just in the health-care industry, but in the retail industry, the financial industry, and even in the entertainment industry, as we recently saw with a high profile incident.

As we consider the benefits and risks of the new electronic health-record systems being implemented today by hospitals across the country, we must keep everything in perspective. And that perspective is one of the world we live in being continually connected, continually on the move, and continually enabled with critical life-saving information at the location it is needed.

Rob Faix is a principal with Impact Advisors, a health-care IT consulting firm based in Illinois.

Be social

Follow us at **@OrlandoOpinion**

Like us at **facebook.com/orlandoopinion**

At OrlandoSentinel.com/opinion: Look for editorial cartoons from around the country, Today's Buzz question, 30-Word Rant and national columnists, as well as editorials, letters to the editor and guest columns you may have missed.

The Needle

"Starbucks is offering a limited number of sterling silver gift cards that cost $200. They say it's a very classy way of saying, 'I know nothing about you.'"
— Jimmy Fallon

"Conversation with Uber driver most meaningful social contact of area man's life"
— Derf Magazine

"Scientists say they're closer to developing a pill to replace exercising. Americans said that it better come in cool ranch flavor."
— Conan O'Brien

DANA SUMMERS/TRIBUNE CONTENT AGENCY

HOME DELIVERY RATES

SUBSCRIPTION RATE PER WEEK, BY CARRIER			
7-day	Wed-Sun	Fri-Sun	Sunday
$9.52	$7.41	$5.30	$4.31

TO SUBSCRIBE, CALL 407-420-5353

E-EDITION AND DIGITAL COMBO
$9.99
5-weeks

All subscriptions may include up to four Premium Issues per year. For each Premium Issue your account balance will be charged an additional $1.00 in the billing period when the section publishes. This will result in shortening the length of your billing period. Premium Issues scheduled in 2014: The Envelope on 3/2; Explore Florida on 5/18; Football Preview on 8/24; Thanksgiving Day Edition on 11/27. Subscription types other than 7-day may also receive, at our discretion, the following issue as part of their current subscription in 2014 – 11/28. Vacation holds do not extend your expiration date.

All carrier prices include transportation and applicable Fl. sales tax. Member of Alliance for Audited Media.

A Tribune Publishing Company, LLC. USPS 412100, ISSN 0744-6055. Published every morning by Orlando Sentinel Communications Company, LLC, 633 N. Orange Ave., Orlando, FL 32801. Periodical postage paid at Orlando, FL POSTMASTERS. Send address changes to Orlando Sentinel, PO Box 2833, MP224 Orlando, FL 32802. For customer service call, 1-800-359-5353