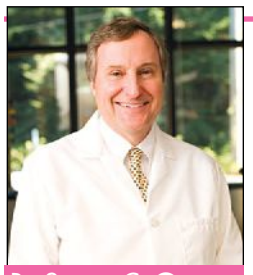
PHYSICIANSNEWS

PhysiciansNews.com FALL 2013 Digest



By Steven C. **Quay**, M.D., Ph.D., FCAP

TAKING AIM AT BREAST CANCER
with Pre-Cancer Treatment

Women have consulted with their physicians for generations to gain insight about the risks of breast cancer and to educate themselves about the optimal protocol for early detection and treatment. Unfortunately, this aspect of the doctor-patient relationship is rendered more complex by the absence of very accurate, safe and reliable testing methods. Some physicians persist in believing that mammograms offer the ideal option. However, female patients are justified if they are bewildered by the controversy that hangs over the accuracy of mammograms and how often they ought to be administered.

In the absence of more accurate tools for early breast cancer detection, a modicum of uncertainty is destined to persist. Tools of greater accuracy are also needed because the sooner physicians are capable of detecting breast cancer in their patients, the greater the range of available treatment options.

This problem raises the question of what sort of role technology might play in the solution. As it turns out, steps are underway at Seattle-based Atossa Genetics, Inc. to commercialize its recently developed, FDA-cleared diagnostic device that can be used to painlessly collect samples that are then be tested in Atossa's wholly-owned laboratory. The test can identify women with reversible, pre-cancerous changes that place them at high risk of future breast cancer, and then offer them a treatment for the precancerous changes before they become malignant.

The test, named the ForeCYTE Breast Health Test, entails the use of an FDA-cleared, patented device, resembling a breast pump in appearance, that collects nipple aspirate fluid for cytological testing in women between the ages of 18 and 73. The fluid collected in this way can be used in the determination and/or differentiation of normal versus premalignant versus malignant cells. The procedure is noninvasive, virtually painless for the patient, and takes only about 10 minutes to perform. The collected specimens are subsequently tested in Seattle, WA at the National Reference Laboratory for Breast Health, a subsidiary

See Taking Aim on page 2

By Patricia A. **Costante**

IS THERE A DATA BREACH
IN YOUR PRACTICE'S FUTURE?

Did You Know… that the number of people falling victim to identity theft has more than doubled since 2003? In 2003, five million people were victims of identity theft. In 2012, that number jumped to 12.5 million. And the number of people affected by data breaches in the U.S. continues to climb each year.

In the prior decade, most data breaches were caused by human error (such as lost devices or records being exposed in insecure ways). Now, breaches have become more targeted and sophisticated with a large and growing number of breaches being caused by hackers and cyber criminals. Because data can now reside in multiple locations, including unsecured smartphones, laptops and tablets, and can be transported to an infinite number of locations, thieves have more areas to target. Most experts agree that the problem of data breaches will get worse before it gets better, with breaches expected to become not only more frequent, but also more severe.

There is also more awareness of data risk than there was a decade ago, thanks in large part to the Health Insurance Portability and Accountability Act (HIPAA), the HITECH Act, the Red Flags Rule and state data breach notification laws that require disclosure and corrective action by healthcare organizations.

How Much Does a Data Breach Cost a Practice?

A data breach at even a small physician practice could easily run into the hundreds of thousands of dollars — enough to cripple a practice running week to week financially. Some expenses physicians can expect to incur when a breach occurs include legal fees, IT forensic costs, notification costs, credit monitoring costs, public relations expenses to salvage patient goodwill and advertising expenses to make the public aware of the steps that have been taken to address the breach. There may also be significant penalties assessed against a practice involved in a data breach, which may range from $100 to $50,000 per violation. The Department of Health and Human Services' Office for Civil Rights has made clear that no practice is too small to be fined.

Are You Complying With the Latest Requirements?

Physicians are becoming

See Breach on page 2

PRST STD
US Postage Paid
Permit No. 397
Bellmawr, NJ

INSIDE THIS ISSUE

POLICY

POLICY

LAW

DEPARTMENTS

Taking Aim from Page 1

of Atossa Genetics. If required, precancerous changes can be addressed with lifestyle intervention or pharmaceutical treatment. For example, in women with atypical hyperplasia, lifestyle changes have been shown to reduce future risk of breast cancer by as much as ten percent and treatment with tamoxifen produces a reduction of greater than 80 percent in the development of future breast cancer.

Ultimately, the precancerous changes may be treated with intraductal therapy that is also being developed by Atossa. The therapeutic system, which is currently in the research phase, will provide pharmaceutical formulations that can be introduced into a "sick duct" with an FDA-cleared microcatheter to treat the cancerous condition or reverse the pre-cancerous changes before they turn malignant. This technique avoids treating the entire patient with powerful and toxic drugs; instead, it acknowledges that the problem lies with a milk duct that is two inches in length and the diameter of a strand of angel hair pasta.

Atossa is foreseeing additional technologies for improved treatment of breast cancer. For example, one test, intended for survivors of breast cancer, offers preliminary warning about the presence of circulating breast cancer tumor cells in a simple "liquid biopsy" blood specimen. The test identifies these cells and can be harnessed directly after a woman starts breast cancer therapy, or at the time of diagnosis or biopsy, in order that she and her healthcare provider can make more informed decisions about effective options for treatment. The test could also be used for recurrence monitoring and whenever a treatment decision needs to be made.

A further test currently under development by Atossa employs genomic analysis to offer insights to enhance the effectiveness of breast cancer treatment for women who have early-stage breast cancer. This test provides genomic evaluation of risk for recurrent breast cancer and therapy selection, evaluating a greater number of genes for more informed patient management. The report generated by this test indicates the potential for cancer recurrence and offers a personal profile that can help pinpoint the ideal course of treatment.

If Atossa's technologies are successful, with precancerous changes diagnosed during routine checkups and then treated immediately afterward, female patients who are at risk for breast cancer might be given a safer and more dependable route to long-term health.

Steven C. Quay, M.D., Ph.D., FCAP is Chairman, President and Chief Executive Officer of Atossa Genetics, Inc. and Director of the National Reference Laboratory for Breast Health. He can be reached at Steven.Quay@AtossaGenetics.com

Breach from Page 1

increasingly aware that compliance with regulations like HIPAA is imperative. While training and preparation of compliance plans is something many practices can accomplish, there remains a challenge to control the multitude of data found on laptops, smartphones, memory sticks, human resources systems and other devices that are used in day-to-day operations of a medical practice.

Physician practices have until September 23, 2013, to become compliant with a final set of HIPAA federal privacy rules. Under the new rules, doctors now must assume the worst-case scenario in the event of a possible privacy breach. Previous regulations had required a practice to notify affected patients and the federal government only if it determined that a breach involving patient records had occurred and that it carried a significant risk of financial or reputational harm to patients. The new rules eliminate that standard, and replace it with a stricter one. Now, any incident involving patient records is assumed to be a breach, and unless a practice conducts a risk assessment that proves a low probability that any protected information was compromised, the breach must be reported. This new standard is expected to result in many more official reports of breaches, as well as additional work and costs to physician practices. (For the full rule, go to www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

HIPAA typically has focused on healthcare professionals, health plans and other entities that process health insurance claims. But because some of the largest security breaches have involved healthcare providers' business associates, many of the law's requirements were extended to these entities as well as their subcontractors. For physicians, a business associate may be any firm that handles patient data, such as a storage provider, a shredding company or a benchmarking firm that measures physician performance. With contractors becoming as fully liable as everyone else affected by HIPAA, physicians' offices are going to take on additional legal responsibilities. For example, if someone paid to shred patient files instead throws the documents into a trash bin and causes a breach, the practice also is subject to enforcement violations caused by that business associate. Although the rules specify September 23 as the compliance date for the new regulations, healthcare professionals have an extra year to revise existing business associate agreements to become compliant.

Additionally, physicians need to stay abreast of new risks that are identified as needing attention. For example, the Department of Health and Human Services now wants photocopy machines examined as part of data security. Physician practices need to make sure that all personal information is wiped from hardware before it is recycled, thrown away or sent back to a leasing agent. For more information on safeguarding sensitive data stored in the hard drives of digital copiers, go to http://business.ftc.gov/documents/bus43-copier-data-security.

Are You Adequately Insured Against Data Breach Risks?

Physicians will certainly continue to work hard to assure compliance and prevent protected health information breaches. Unfortunately, however, even the best prepared practices may not be able to prevent a breach from occurring. Consequently, every practice should have a plan in place regarding how best to handle a breach if it does occur and must be cognizant of the potentially high financial cost that comes with a breach.

Many organizations now consider cyber security threats to be as big as — or bigger than — the threat of a natural disaster or fire. Just as those organizations carry insurance for the relatively small chance that a tornado or fire destroys their businesses, many now are looking at policies that will cover the potentially devastating impact of a data breach. There are specialized insurance products available that are directed at the healthcare provider market and address the particular liabilities faced by physician practices.

Even though data security insurance can be quite inexpensive, particularly when compared to the average claims paid out, physicians often do not pay as much attention to this type of coverage as they should. To many physicians who are busy maintaining their practices while installing electronic health records and meeting the requirements of meaningful use, weighing the options of data security insurance may feel overwhelming. Yet as more and more breaches are publicized, along with the amount of associated fines, more practices are working with their brokers to make sure they are managing their data security risks adequately. At the very least, physicians should look deeper at their existing coverage to see what, if any, of these types of risks may be covered by their liability insurance policy. The peace of mind that comes from adequate protection will be well worth the investment.

Patricia A. Costante is Chairman and CEO of MDAdvantage Insurance Company of New Jersey.