PROTECTING PATIENT HEALTH INFORMATION:

A Different Kind of Fight for Cancer Centers and Oncology Practices

Cyberattacks involving the theft and sale of personal information are rising every year. Healthcare is now the number one target for these attacks due to the value of the information contained in protected health information (PHI).[1] Stolen patient information includes confidential personal health backgrounds, social security numbers, bank details and family histories. Medical files, billing and insurance records contain the most valuable patient data and are most often successfully targeted.[1]

As cyberattacks increase in number, they also become more sophisticated and difficult to prevent. The kinds of attacks that criminals are using against healthcare organizations are continuously evolving. They include the theft of patient records, malware, ransomware, denial of service, spear phishing (email fraud), and more. These attacks can have a devastating impact on healthcare organizations, patients and their families.

For healthcare providers, the problem is real. And it's getting worse.

For healthcare providers, being hit by an attack involving the theft of confidential patient information is a matter of *when* not *if*. The statistics on security breaches at health-care organizations over the past several years make for sobering reading.

According to a 2016 study, nearly 90 percent of healthcare providers had been hit by data breaches in the previous two years.[2] Unfortunately, attacks are up on all fronts—including theft of patient records and ransomware—and cybercriminals continue to find new ways to breach information security. More than 94 million individuals were affected by breaches at healthcare organizations during the first six months of 2015. This represents a 20-fold increase compared to all of 2014.[3]

The costs are devastating. Not just for healthcare organizations, but for patients too.

The economic, business and personal costs of healthcare information security breaches are substantial—for the healthcare industry, for individual healthcare providers, and especially for patients and their families.

As of 2016, the total financial cost of data breaches to the healthcare industry is estimated to be as high as $6.2 billion annually.[2] For healthcare provider organizations including cancer centers and oncology practices, the average cost of a data breach in 2016 is estimated to be more than $2.2 million.[2]

Of course, the damage done to healthcare organizations by a data breach goes far deeper than the immediate cost of the incident. Audits by the Office of Civil Rights (OCR) and having the details of a major patient information data breach published online on OCR's online breach reporting portal can cause irreparable damage to an organization's reputation. Moreover, these data breaches cause further damage to these organizations by distracting management. The process of notifying shareholders, regulatory authorities and patients that a breach has occurred is difficult enough. Having to plan and implement corrective actions and dealing with the public response to a data breach takes an enormous amount of administrator and physician time away from what should be every healthcare organization's number one priority—delivering high quality care to patients.

The cost to patients of having their medical identity com-promised is even worse, both emotionally and financially, because they are already vulnerable. Many of those under-going treatment for cancer are fighting for their lives. They are worried about the well-being of their families. Many of them are concerned about their ability to afford treatment. The last thing a cancer patient should have to worry about is having their health information compromised and having to deal with the aftermath.

According to research on the devastating impact of medical identity theft to the healthcare industry and patients, the average monetary cost to a patient of a data breach was approximately $13,500.[4] This includes the costs of restoring credit, reimbursing healthcare providers for fraudulent claims and correcting inaccuracies in their medical records. Sadly, nearly two thirds of healthcare organizations offer no services to their patients to protect them from a data breach.[5]

Most victims of medical identity fraud believe they suffered a negative impact on their reputation, often causing considerable embarrassment by having their medical conditions – present or past – divulged to third parties. Research conducted in 2015 found that almost a fifth of those victimized by medical identify fraud believed they had missed out on career opportunities as a result, while three percent attributed lost employment to the theft.[4]

This is a different kind of fight for cancer treatment centers and oncology practices.

Cancer centers and oncology practices fight every day to save their patients' lives and give them hope in the face of a terrible disease. Protecting the security of patient information is a different kind of fight; one that healthcare organizations must take seriously in order to protect their patients. This is an area where, according to information security experts, healthcare providers can improve.

"Many organizations just want to meet HIPAA (Health Insurance Portability and Accountability Act) requirements in the most minimal fashion without giving much thought to the consequences of a major breach," said Raymond Sias, a healthcare information security analyst and trainer from El Paso, Texas.[6] "It's not a matter of *if,* but *when* a data breach will occur, and organizations that don't put the necessary resources into place to protect patient information can expect very bad consequences from regulatory agencies, lawyers and the public," he added.

Vast amounts of sensitive patient information reside today in the modern healthcare provider network, and these are increasingly targeted by "bad actors" such as hackers and other criminals who exploit vulnerabilities in these networks. Oncology departments, cancer treatment centers and community oncology practices need to focus on helping their patients fight cancer, and cancer patients should not have to add to their burden by having to be concerned about their sensitive information being stolen. Consequently, cybersecurity has become a top priority for Varian.

As a result, major security-oriented improvements are being engineered into Varian's product portfolio. We anticipate rolling out the first of these during 2016. Some of the security enhancements will be evident to clinicians while others may only impact customer IT or be altogether transparent. At Varian, we are committed to state-of-the-art software and cutting-edge technologies that treat cancerous as well as non-cancerous tumors. We are also dedicated to helping ensure that patient information is secure and protected from cyberattacks.

For more information, contact: infosec@varian.com

1 Security trends in the healthcare industry. New risks and priorities for keeping patient information safe. IBM Security, November 2015. Available at http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03048USEN&attachment=SEL03048USEN.PDF.

2 Sixth annual benchmark study on privacy and security of healthcare data. Ponemon Institute LLC, Sponsored by ID Experts, May 2016. Available at https://www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm_source=Referral&utm_medium=press%20release&utm_campaign=Ponemon%202016.

3 Cybersecurity in healthcare: a time to act. Fidelis Cybersecurity, September 2015. Available at https://www.fidelissecurity.com/resources/cybersecurity-healthcare-time-act.

4 Fifth annual study on medical identity theft. Ponemon Institute LLC, Sponsored by the Medical Identity Fraud Alliance with support from: Kaiser Permanente, ID Experts, Experian Data Breach Resolution and Identity Finder, LLC, February 2015. Available at http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf.

5 Fifth annual benchmark study on privacy and security of healthcare data. Ponemon Institute LLC, Sponsored by ID Experts, May 2015. Available at https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data.

6 Protecting patient identifiable information in the world of radiotherapy. Varian Medical Systems, May 27, 2016. Data on file, Varian Medical Systems, Inc.

VARIAN medical systems | A partner for **life**

USA, Corporate Headquarters and Manufacturer
Varian Medical Systems
Palo Alto, CA
Tel. 650 . 493.4000
varian.com

EMEIA and CIS Headquarters
Varian Medical Systems
International AG
Cham, Switzerland
Tel. 41 . 41.749.88.44

Latin American Headquarters
Varian Medical Systems
Brasil Ltda.
São Paulo, Brazil
Tel. 55 . 11 .3457.2655

Asia Pacific Headquarters
Varian Medical Systems
Pacific, Inc.
Kowloon, Hong Kong
Tel. 852.2724.2836

Australasian Headquarters
Varian Medical Systems
Australasia Pty Ltd.
Sydney, Australia
Tel. 61 .2 . 9485.0111

RAD 10421 07/2016