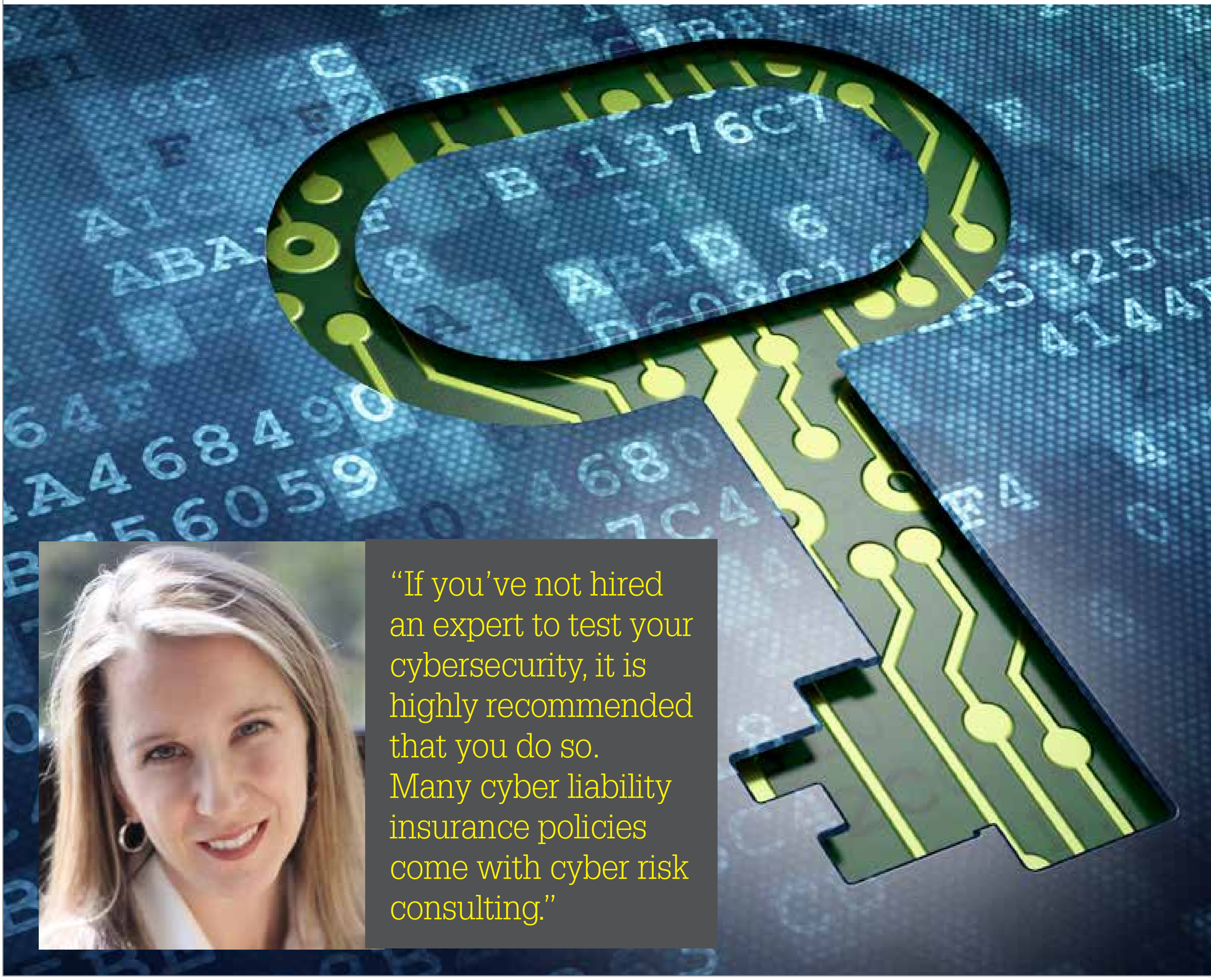
PRIVACY BREACHES: BEWARE

No healthcare organization is safe from data breaches, and as cyberattacks become more sophisticated, it becomes increasingly important for consumers to stay one step ahead of the perpetrators. Michelle Foster Earle, president of OmniSure Consulting Group, offers her advice.

Although no patient data were breached, Healthcare.gov was hacked on September 5, leaving many healthcare organizations wondering if hackers might get into their system too. On August 18, it was reported that Chinese hackers had harvested the personal data of 4.5 million patients served by Community Health Systems (CHS), which is the largest reported cyberattack to date.

Robert Wah, MD, new president of the American Medical Association, warned healthcare providers and other organizations to prepare for a breach on a similar scale to the one that affected millions of Target's customers in December 2013. Health data stewards are in a race against incredibly sophisticated cybercriminals who are motivated by easy money. A health record could bring anywhere from $20 by itself to $1,000 when bundled with other documents that can be used for credit theft,



> "If you've not hired an expert to test your cybersecurity, it is highly recommended that you do so. Many cyber liability insurance policies come with cyber risk consulting."

MAKSIM KABAKOU / SHUTTERSTOCK.COM

identity theft, financial or medical fraud, and even obtaining prescriptions for controlled substances.

Cyberattacks are only one of the ways breaches happen in healthcare. Theft of laptops, improper disposal of paper records, unauthorized access to e-mail or network servers, improper disposal of laptops, mobile devices, and other portable electronics are all reported regularly. Firewalls, routers, and network security for providers present special risks as well.

Just as medical facilities prepare for potential medical errors with patient safety initiatives and medical professional liability insurance, it's important to prepare for the potentially devastating impact of a data breach. If you've not hired an expert to test your cybersecurity, it is highly recommended that you do so. Many cyber liability insurance policies come with cyber risk consulting. Get an expert opinion.

In the meantime, you can use the table below and on the next page as a preliminary checklist* for auditing your data security. ■

*The checklist has been formed from information provided by the Commonwealth of Massachusetts for the following article: 201 CMR 17.00: *“Standards for the Protection of Personal Information of Residents of the Commonwealth”* http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

CRITERIA	YES	NO
Safeguards are appropriate for the following:		
A comprehensive information security program that contains administrative, technical and physical safeguards		
The size, scope, and type of business		
The designated staff under the security program		
The resources available		
The amount of stored data		
The security and confidentiality of both the customer and employee		
Unauthorized access is tested at least monthly		
Encryption software is current and loaded on all appropriate computers		
Malware protection is updated at least monthly		
Personnel		
At least one or more employee is are designated to maintain the information in the program		
Disciplinary procedures are in place for violations of program rules		
Terminated employees are prevented from accessing computer records		
Employees are required to change passwords at least annually		
Employees are trained in the proper use of the computer security system		
Training is provided for both employees and contract personnel		
Employees are tested on the system to establish competency		
Employees sign a confidentiality agreement that includes the following: ▪ Passwords ▪ Trade secrets ▪ Data ▪ Systems information		
Background checks are conducted upon hire and annually thereafter		
Personnel are trained to avoid opening suspicious attachments		
Staff members are prohibited from accessing social networks on company computer systems		
Staff members are prohibited from accessing websites outside of their job requirements		
Staff members are prohibited from downloading software without express permission from management		
Staff members are prohibited from taking computerized patient data from the facility		
Staff members are prohibited from taking laptops containing confidential data from the facility		
Security program		
Ongoing evaluations include at least an annual check on all systems		
Annual assessment of the accuracy of policies and procedures		
Systems are in place to detect security system failures		
Annual audits are conducted to verify that third-party service providers maintain appropriate security measures to protect personal information.		

Other helpful resources

Health Breach Notification Rule:

http://business.ftc.gov/privacy-and-security/health-privacy/health-breach-notification-rule

Health Information Privacy Training and Tools: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/

Mobile Devices: http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Michelle Foster Earle is the president of OmniSure Consulting Group, a risk management firm contracted by some of the nation's leading medical professional liability insurance companies to help medical practices, hospitals, healthcare facilities, and providers of healthcare and social services nationwide reduce risk, improve performance, and avoid lawsuits. She has earned designations in healthcare management, is a licensed General Lines Property and Casualty agent in Texas, and is an Associate in Risk Management.

CRITERIA	YES	NO
Policies are in place pertaining to the following: ▪ Storage ▪ Access ▪ Transportation of records that pertain to personal information ▪ Data recovery in case of emergency ▪ Deletion of personal information		
Systems are in place to identify and assess security risks		
Internal and external risks are assessed at least weekly		
Systems are in place to verify confidentiality protections		
Safeguards are in place to restrict access to records that contain confidential data		
Storage of printed data is kept in secured areas		
The security system is monitored daily		
Security measures are evaluated when material business practices change		
Security breaches are documented		
Responses to security breaches are documented, tracked, and trended		
All data are encrypted when transmitted across public networks		
Unauthorized access is identified and prevented		
Firewall protection is authenticated monthly		
Antivirus protection is updated at least monthly		
Antivirus protection updates are provided by the vendor when threats are detected		
Systems are in place to prohibit staff from taking confidential data from the workplace		
Authentication protocols		
Authentication protocols, including date of current protocol, are in place		
User ID and identifier protocols are followed		
Method for assigning passwords is current and accurate		
System passwords are retained in a central, secured area that is only accessible to management		
Access is restricted to active users only		
Off-site authentication is controlled and limited by policy		
Access is blocked after multiple unsuccessful attempts to gain access		
Access is governed by users' job descriptions		
Access is restricted to those who need the information to complete their jobs		
Default passwords are issued by employees, not vendors		
Password criteria are used when employees choose their own passwords		
Unauthorized use of company systems is tracked and reported		