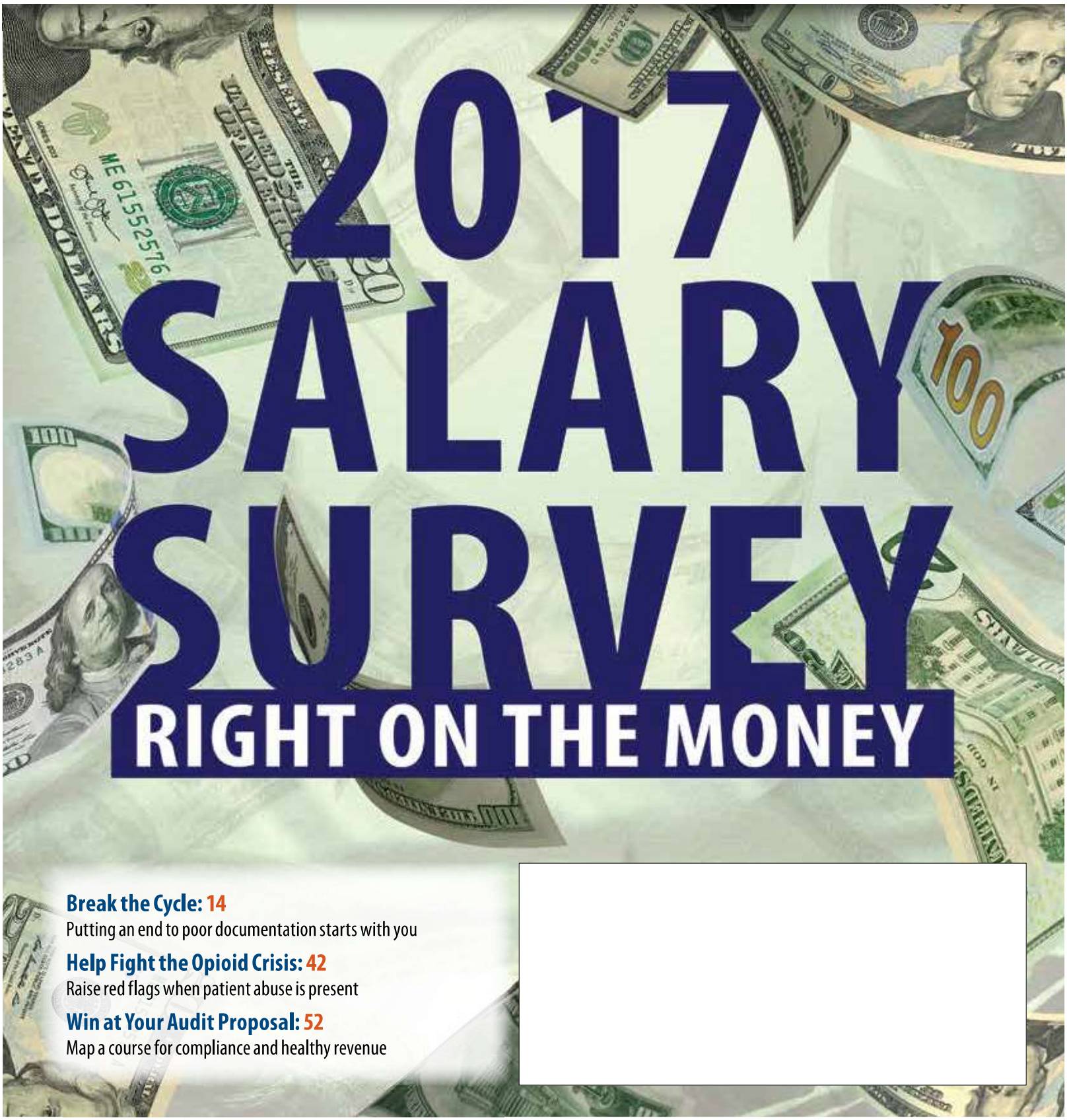
HEALTHCARE BUSINESS MONTHLY

Coding | Billing | Auditing | Compliance | Practice Management

AAPC®
Advancing the Business of Healthcare

February 2018 www.aapc.com



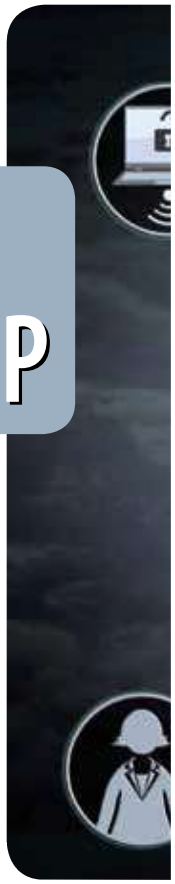
2017 SALARY SURVEY

RIGHT ON THE MONEY

By Brian Shrift, CISSP, HCISPP, CRISC, CISA

3 IT SECURITY MEASURES YOU CAN'T AFFORD TO SKIP

Your practice's livelihood and your patients' privacy are at stake.



Information technology (IT) security is comparable to cancer: Just as there is no "silver bullet" to prevent cancer, there is no single product to protect against every security threat. And just as you can reduce the risk of cancer through healthy habits (e.g., don't use tobacco, eat a healthy diet, exercise regularly, etc.), you can reduce IT security risks by implementing proper controls or safeguards.

MITIGATION IS THE GOAL

The goal of IT security is to mitigate the risk of an "incident." An incident is anything that affects the (i) confidentiality, (ii) integrity, and (iii) availability of protected health information (PHI).

Safeguards must be in place to protect patient information from:

- Unauthorized access and disclosure;
- Improper alterations or deletions; and
- Being inaccessible when needed.

Here are my top three IT security recommendations for healthcare organizations, which are all HIPAA Security Rule requirements.

1. Backup and Disaster Recovery Plan

If your practice suffers an incident, you must be able to recover your patient files. If patient files are lost, you may not be able to recover your practice. A backup and disaster recovery plan is not only a HIPAA Security Rule requirement, it's good business practice.

Consider these three key elements when selecting a backup solution:

1. Offsite and Encrypted – A backup is a centralized copy of all your data, possibly from multiple systems. It's extremely important for you to back up data leaving your office on media (disk, USB drive, tape, etc.) using encryption. If you're using an online backup provider, the transmission from your practice to that vendor must be encrypted, as well. You also must have a Business Associate Agreement on file with the vendor, and the vendor must protect your data to HIPAA Security Rule standards.

2. Image Backup – Data backups protect your important data, such as documents, patient files, databases, etc., but it's considered the bare minimum. An Image backup — an identical copy, or image, of your server or system — is also recommended.

In the event your system suffers an incident that requires system restoration (such as an operating system error, failed windows patch, hard drive corruption, ransomware attack, electrical surge, etc.), you won't have to rebuild the system from scratch if you can simply restore the image. This will save countless hours of downtime and technician labor. A good backup solution is one of the most cost-effective safeguards you can put in place.

3. Monitored and Tested – It's vital to monitor and test your backup solution. Do not assume a solution that worked 11 months ago still works today. Monitor backups daily, and conduct a full backup and disaster recovery test annually. For example, an IT professional can restore your IT system to loaner hardware, documenting any issues discovered and how long it took to restore your system. It's essential (and reassuring) to know that your backup is working properly and exactly how long it will take to restore your system in the event of an incident.

2. Security Awareness and Training

Employees are often a company's most expensive resource. From an IT security perspective, they are usually the biggest security risk, as well.

Security awareness and training is the process of educating employees on computer security and good computing practices. Investing in education, such as teaching what a phishing attack is and ways to avoid falling victim to them, is part of security awareness and training.

Office of Civil Rights' guidance is clear: If your system is infected with ransomware, it's a breach and is reportable. If you have more than 500

iStockphoto/LeoWolfert

patient records affected, your practice is about to make the local news. Ransomware affects thousands of systems daily, and is often caused by employees clicking emails or links they should have ignored, or better yet, reported. The chance of compromise dramatically increases if you don't have the proper safeguards in place.

It's the burden of the practice to conduct a forensic audit to determine if the ransomware attack transmitted data (PHI) outside of your network or if it only encrypted the data (making it inaccessible).

3. Regular Maintenance

Another critical part of your IT security plan is to ensure regular maintenance and software patching occurs. Much of the malware, ransomware, and other attacks are against known vulnerabilities in systems that have gone unpatched. The recent Experian breach is a perfect example of an attacker targeting a website vulnerability. Sadly, this may have been prevented if Experian's IT staff applied the patch for this vulnerability, which was released two months prior to the attack.

Along with applying patches to computers, servers, and applications, ensure all other IT system components are maintained. Maintenance can be as simple as checking a log on a regular basis (such as a backup log) or checking to ensure your anti-virus program is updating and scanning regularly. Updating the firmware on network devices, such as your firewall, addresses vulnerabilities and usually enhances capabilities or performance. A required maintenance task is a regular review of audit logs to ensure PHI is accessed appropriately. Don't forget about your mobile devices and apps, as they have regular software security updates, as well.

A good backup solution is one of the most cost-effective safeguards you can put in place.

Take a holistic approach to IT security for your practice. You can't just focus on one area of IT security. To reduce risk, implement multiple safeguards that work together to keep your systems healthy. **HBM**

Brian Shrift, CISSP, HCISPP, CRISC, CISA, is an IT security professional and HITRUST Certified CSF Practitioner, specializing in small and medium organizations. He works with clients daily, providing advice and counsel to help them strengthen the security posture of their organization.

Resource

There are several resources available. For example, Brian's firm offers a free online Security Awareness & Training course. Go to **www.PrecisionBS.com** and select "Education." Look on the internet for others or consult your IT professionals."