Cyber Security

What's the "new normal" of health information security?

If the speed of new threats emerging isn't enough to pique your interest in this topic, we're convinced the vast number of individuals whose health data has already been compromised will. (It's nearly 135 million individuals affected since 2009, by the way.[1]) Highly skilled adversaries continuously develop new techniques to access information, with motives ranging from fraud to cyber espionage for political and economic purposes. Sadly, data breaches at organizations handling protected health data probably aren't going to end any time soon. That makes it a great time to better understand the topic and determine what more you can do to help protect your population's data. You can play a critical role in driving security measures of protected health data in your organization.

What is cyber security?

Cyber security is the set of practices, processes and controls that protect information on electronic devices, such as computers, smartphones and computer networks. Protections are typically based on the level of sensitivity or risk represented by the information asset.

Looking for more? *Click here* for an overview of cyber security by the U.S. Department of Homeland Security (4/15).

If you aren't sure where to start, consider these five important new realities we're facing in the world of health information security:

1. It's a new world of constant threats
2. Health organizations are in the crosshairs
3. New threats are emerging at warp speed
4. Privacy is inextricably linked to information security
5. It's time to do things differently

Let's take a look at how each of these five things is defining the ever-evolving health information security challenge.

[1] *Breaches Affecting More Than 500 Individuals, numbers through 6/1/15, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.*

1 It's a new world of constant threats

Consider the floodgates open. A barrage of new threats to health information security is emerging due to a new and complex landscape. This new terrain is characterized by:

a. **Sophisticated and organized cyber criminals who have emerged across the globe:** Larger, more organized criminal organizations have formed to create the highly effective "professional criminal."

b. **Geopolitical forces — attacks on private health care companies are increasingly state sponsored:** Some are dubbing it a new kind of "cold war" – nations the world over are hiring and training hackers (in some situations, numbering in the thousands) to be deployed in cyber-attack activities. From cyber espionage to targeted attacks on U.S. companies (as in the Sony Pictures Entertainment attack), we're likely to see more of these activities as nations further develop these capabilities.[2]

c. **Proliferation of mobile devices has increased the scope of security issues and protections needed:** Nearly two-thirds (64%) of American adults own a smartphone today. That number is up from 35% in the spring of 2011.[3] Any guesses which way that trend is expected to move in the future?

[2] *"Sony and the rise of state-sponsored hacking," CNET, 12/14, accessed 6/1/15.* http://www.cnet.com/news/sony-and-the-rise-of-state-sponsored-hacking/.

[3] *Aaron Smith, "U.S. Smartphone Use in 2015," Pew Research Center, Washington, D.C., 4/15, accessed 6/1/15.* http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

More than half of smartphone owners have used their phones to get health information and do online banking

% of smartphone owners who have used their phones to do the following last year:

Pew Research Center American Trends Panel Survey, October 3 – 27, 2014, Pew Research Center.

THE TAKEAWAY

Cyber attacks aren't likely to stop any time soon, so buckle up. In fact, the landscape will continue to evolve, so staying abreast of changes will be critical in continuing to understand and address these risks effectively.

2 Health organizations are in the crosshairs

Wondering about Aetna's information security strategy? *Click here* for an infographic outlining our cutting-edge approach.

Any organization that handles a high volume of personal data is of particular interest to cyber criminals. And, health organizations (health care systems, health benefits companies, health data companies, etc.) **have an abundance of this data in their systems** (names, Social Security numbers, birth dates and more). **Criminals can easily resell this information** for a profit on the black market.

But even more concerning…nation state sponsored threat actors with deep technical resources are **harvesting consumer information** from health care providers and payers. Based on the last four health care attacks that were publicized, they are using big data analytic techniques to target employees of companies of interest.

Many attackers mine health and other personal information to improve the success rates of their phishing emails, among other things. How? They include this information in their emails to entice someone to open an email or click on a link they may have otherwise realized to be illegitimate. (More on phishing later under #5.) **Phishing is the technique of choice for nation states and profit motivated threat actors.**

THE TAKEAWAY

Since 2009, as much as 42% of the U.S. population has faced some sort of data breach of their personal information.[4] Organizations handling health information need to take swift action to protect their patients' and members' data. The wealth of data held by these organizations is a serious enticement to criminals all over the world.

[4] *Breaches Affecting More Than 500 Individuals, numbers through 6/1/15, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.*

3 New threats are emerging at warp speed

For you non-Trekkies out there, warp speed means "insanely fast." The rapid pace of technology change, increased accessibility of data and the unrelenting focus of cyber criminals on breaking through security protocols are all **easily outpacing regulatory changes**. Just consider the rush we're seeing in Congress to push forward legislation to regulate drone activity. The rate of innovation has been escalating in recent years, opening new doors before the old ones are shut.

What's driving the warp speed? Some contributing factors were mentioned previously under #1 and #2 (highly organized criminals, proliferation of mobile devices, etc.), but consider this change as well:

Increased accessibility of data

a. **Increased connectivity via the Internet of Things** (objects such as biometric monitors and devices, with sensors that have the ability to communicate remotely).

b. **Increased use of cloud-based services.**

c. **New technologies:** Mobile devices are part of the dramatic change, but there's more to this than you might think. High-precision location sensing and motion-processing features, as well as beacons…all of these and many more innovations serve to expand our digital (and physical) footprint…and track it over time.

d. **Increase in electronic medical records.**

The real concern with threat escalation: The changes occur too quickly for the legislative process to keep pace. We can't afford to wait for legislators to pass laws that define how we should respond to new threats. **Political solutions to cyber security risks are in their infancy, so it's important that we learn to quickly adapt to address them ourselves.**

THE TAKEAWAY

The increased frequency and scope of attacks on cyber security are real. We can't wait for regulations to change before taking action. A good policy is to understand the shifting threat landscape and adjust information protection controls consistently to detect and respond to cyber attacks. One way to strengthen your approach — work with strong partners who are more effective in protecting the information of your workforce and/or customers. (See more under #5 — It's time to do things differently.)

How you can protect your privacy on a mobile device

Indeed, there seems to be no limit to what you can do today with a smartphone. From fitness tracking to one-click payments to personal assistants to tweeting… it's impossible to list everything. But, let this very point underscore the need to protect your privacy on all of your mobile devices. Here are some of the basics from LifeHack:

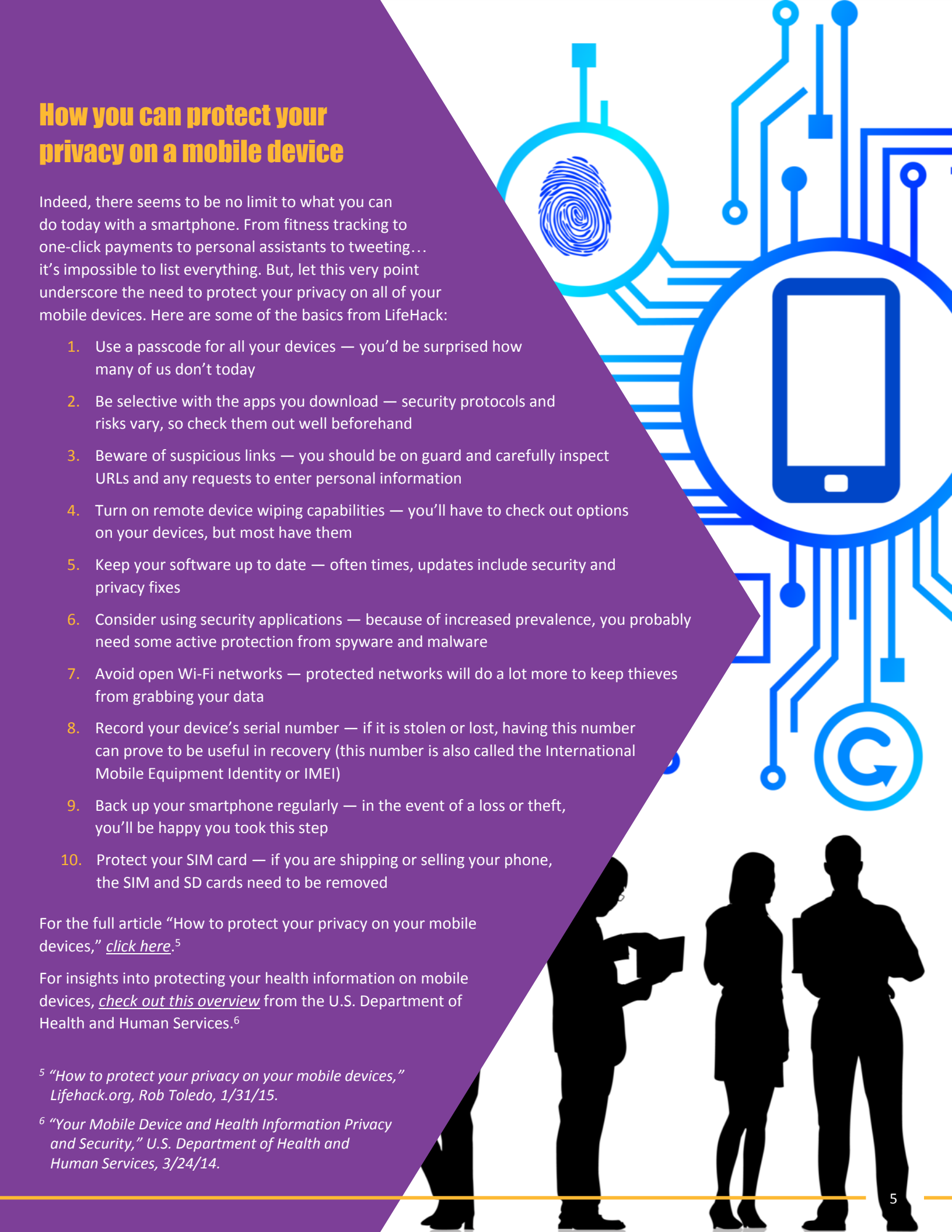
1. Use a passcode for all your devices — you'd be surprised how many of us don't today
2. Be selective with the apps you download — security protocols and risks vary, so check them out well beforehand
3. Beware of suspicious links — you should be on guard and carefully inspect URLs and any requests to enter personal information
4. Turn on remote device wiping capabilities — you'll have to check out options on your devices, but most have them
5. Keep your software up to date — often times, updates include security and privacy fixes
6. Consider using security applications — because of increased prevalence, you probably need some active protection from spyware and malware
7. Avoid open Wi-Fi networks — protected networks will do a lot more to keep thieves from grabbing your data
8. Record your device's serial number — if it is stolen or lost, having this number can prove to be useful in recovery (this number is also called the International Mobile Equipment Identity or IMEI)
9. Back up your smartphone regularly — in the event of a loss or theft, you'll be happy you took this step
10. Protect your SIM card — if you are shipping or selling your phone, the SIM and SD cards need to be removed

For the full article "How to protect your privacy on your mobile devices," *click here*.[5]

For insights into protecting your health information on mobile devices, *check out this overview* from the U.S. Department of Health and Human Services.[6]

[5] *"How to protect your privacy on your mobile devices," Lifehack.org, Rob Toledo, 1/31/15.*

[6] *"Your Mobile Device and Health Information Privacy and Security," U.S. Department of Health and Human Services, 3/24/14.*



4 Privacy is inextricably linked to information security

Since the breach of one can lead to a breach of the other, you can't have privacy without information security. **There is strong interdependency between the two, which requires us to be strong in both areas**:

- A privacy program should be aligned with regulatory requirements at the federal, state and local level (it is also important given the sheer complexity of breach notification requirements).
- An information security program should be driven by threats and risks to enterprise data and be highly responsive to changes to those over time.

The adjustment of existing controls and addition of new controls are the "new normal" because privacy and information security are so closely linked. Adherence to standards alone is insufficient.

THE TAKEAWAY

Strong information security and privacy programs should be top priorities for all organizations in the health care industry. Employers who handle personal data of employees and/or customers have the same responsibility.

Who leads cyber security at Aetna?

Jim Routh is the Chief Security Officer for Aetna and the Board Chairman for the National Health Information Sharing & Analysis Center (NH-ISAC). He is a current Board member for the Financial Services ISAC and an industry thought leader on cyber security resiliency. Jim was a chief information security officer for several large financial services corporations prior to joining Aetna.

5 It's time to do things differently

From protecting information within your own firewall to collaborating with others who protect your employees' and customers' data, it's time to make information security a top priority. What's first on the list?

a. **Ensure that a risk management plan is in place** and is flexible and responsive to the frequent changes of the threat landscape.

b. **Evolve your information classification policy** to identify data, like SSNs, that require a higher level of protective controls than other data.

c. **Shrink the attack surface** by reducing the use and handling of restricted information (e.g., SSNs)

d. **Develop a security culture** (excel at compliance, increase employee awareness of risks, etc.).

e. **Test your incident response capabilities** based on specific scenarios that mimic the evolving threat landscape regularly (at least 4 times a year).

f. **Authenticate your outbound email messages** following the DMARC standard (see infographic).

g. **Involve your supply chain (vendors) and key business partners in your risk assessment and in your response planning;** attackers will often attack a company through a vendor (a recent example is the 2013 Target breach) or other entity that has connectivity into your network.

Cyber crime is indeed a serious and perplexing issue, but you can reclaim at least some of your sanity with the right strategies. In short, prepare for the worst and do what you can to minimize the impact of events when they do occur. Age-old advice that still rings true today.

phishing
[fish ing] [n]

***Phishing** is the illegal attempt to acquire sensitive information, such as usernames, passwords and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.*

Source: Wikipedia

Phishing schemes are a frequent and serious threat to corporations, making employees a critical point of vulnerability.

- Phishing was associated with over 95% of the incidents attributed to state sponsored threat actors.[7]
- 23% of recipients now open phishing messages and 11% click on the attachments in the emails.[7]
- Security analysts at CYREN reported a steep rise in phishing URLs, 3.86 million at the end of March 2015 versus 2.55 million at the start of the year. That represents a 51% increase through the first quarter of the year.[8]

[7] 2015 Data Breach Investigation Report, Verizon.
[8] Q1 2015 Cyber Threat Report, CYREN, 5/15.

10-step plan

Check this *10-step plan* for health information security.

Source: U.S. Department of Health and Human Services (HHS)

Aetna is the brand name used for products and services provided by one or more of the Aetna group of subsidiary companies, including Aetna Life Insurance Company and its affiliates (Aetna).

This material is for information only and is not an offer or invitation to contract. Not all services are covered. See plan documents for a complete description of benefits, exclusions, limitations and conditions of coverage. Plan features and availability may vary by location and are subject to change. Providers are independent contractors and are not agents of Aetna. Provider participation may change without notice. Aetna does not provide care or guarantee access to health services. Health information programs provide general health information and are not a substitute for diagnosis or treatment by a physician or other health care professional. Information is believed to be accurate as of the production date; however, it is subject to change. For more information about Aetna plans, refer to www.aetna.com.