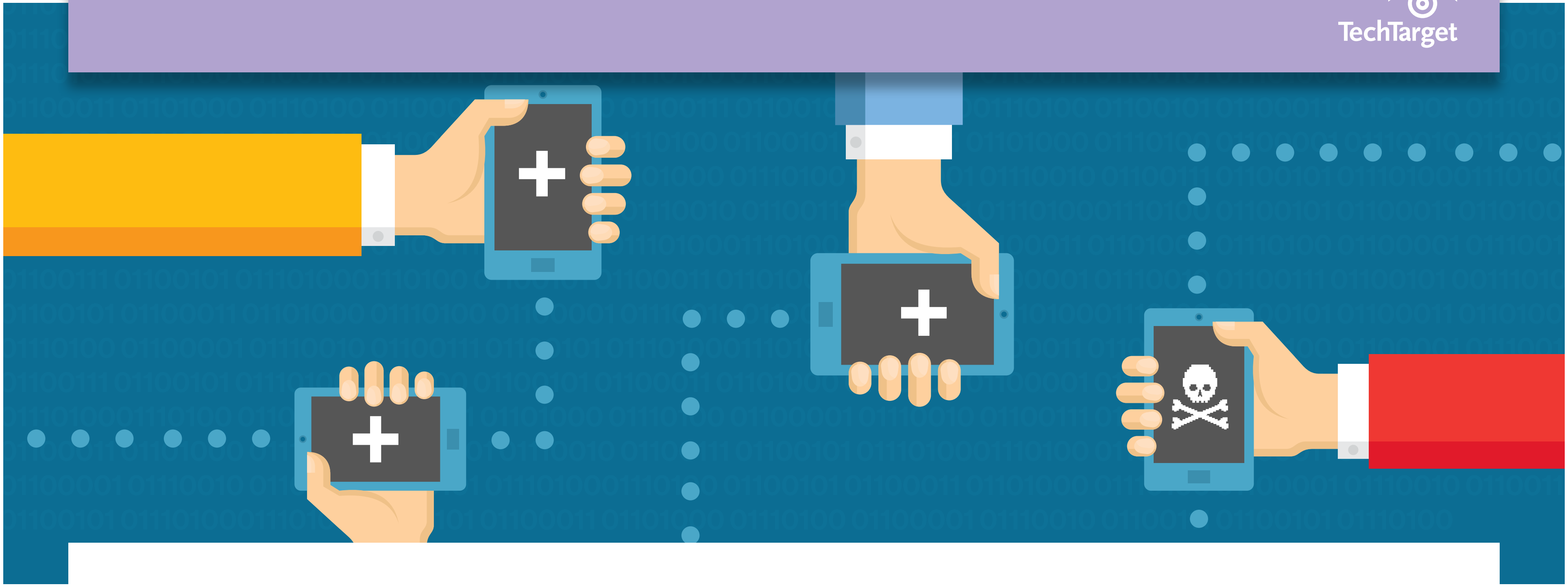

Healthcare Data Security Challenges in a Mobile World

How do you secure patient data in a world on the go? Learn from data breaches others have experienced, experts say, and look at how analytics and artificial intelligence can boost your healthcare data security strategy.

Wanted: Super Sleuth to Help Secure Patient Data

HEALTH IT COULD sure use a modern version of Sherlock Holmes. So many of the efforts behind guarding protected health information and other sensitive patient data involve tracking cybercriminals' paths rather than stopping them with firewalls and encryption.

This handbook looks at the latest security trends for healthcare data security, and it's all perhaps best summed up by this quote from Edward Grogan, vice president and CIO at Calvert Health System Inc., based in Prince Frederick, Md.

"There's amazing concern that with mobile apps and mobile devices [and] Internet of Things that there's less of a focus on quality control and information security development," said Grogan, whose thoughts feature prominently in Kristen Lee's story about learning from past data threats.

Lee brings up an age-old concept: Keep an eye on the weakest link in security measures, including third-party vendors.

Artificial intelligence and data analytics may help track down weak links and breaches into a system, columnist Reda Chouffani discusses in his piece. These two technologies monitor signs of an attack, such as multiple failed password attempts or large amounts of data suddenly being transferred. At the same time, IT needs the skills to decipher these clues.

> So many of the efforts behind guarding protected health information involve tracking cybercriminals, rather than stopping them.

In our final article, Lee returns with an interesting look at how HIPAA—the healthcare law that regulates access to medical records—intersects with wearable devices that monitor health, such as Fitbits. Generally, HIPAA regulates wearable devices only if a covered entity (i.e., a physician) prescribes patients to use such a device. But gray areas always persist with HIPAA, in my experiences.

As health data and mobile health increase in prominence, use technology as your virtual magnifying glass as you and your team—just like Sherlock—act as sleuths stopping cybercrime.

What healthcare data security trends have caught your eye? Let me know by email at swallask@techtarget.com, or on Twitter: @Scott_HighTech. ■

Scott Wallask
News Director, SearchHealthIT
@Scott_HighTech

How Past Breaches Can Inform Future Data Security Plans

WITH DATA THEFT not slowing down anytime soon—consider the recent UCLA health system hack—experts advise IT security professionals to learn from past events in order to bolster their own healthcare data security strategies.

"There's amazing concern that with mobile apps and mobile devices [and] Internet of Things that there's less of a focus on quality control and information security development," said Edward Grogan, vice president and CIO at Calvert Health System Inc. in Prince Frederick, Md. Grogan was one of the experts at the recent mHealth + Telehealth World Congress discussing security breaches and the value of stolen protected health information (PHI).

Kristi Kung, senior associate at law firm Pillsbury Winthrop Shaw Pittman LLP in Washington, D.C., agreed that with more mobile health apps, more mobile devices and more devices being connected to the Internet, there's a greater threat of attack. "Just because you have a secure device does not mean that privacy's always maintained. Any time you're connected to the Internet, you're always susceptible to attackers," she said.

She added that, "the worst is not behind us" and "the healthcare environment isn't as prepared" as other industries.

Grogan and Kung shared ideas on how healthcare organizations can better prepare for mobile health (mHealth) security.

LEARN FROM OTHERS— EVEN THOSE NOT IN HEALTHCARE

Grogan advised attendees at mHealth + Telehealth World to apply lessons from the Target and Heartland Payment Systems Inc. breaches.

In Target's breach, network credentials were stolen in an email malware attack on a third-party vendor that had a supplier portal to the retailer, Grogan said.

"Some of the lessons learned from that breach [are] to consider the weakest link and evaluate third-party vendor security," Grogan said. Other lessons to glean from the Target breach include making sure hospitals incorporate multifactor authentication—where a person must provide two or more credentials to get access to the information—and use network segmentation, where computer networks are split into separate networks.

Grogan said that had Target segmented the supplier network from the consumer network, most likely the breach would not have happened.

He added that containerization would also have helped in this case, in which virtual instances are allowed to share a single host operating system. Organizations can achieve greater security by isolating containers from each other.

In Heartland's case, the payment systems company suffered a data breach in 2008, during which attackers made off with digital information for 100 million credit and debit cards. Heartland also had another data breach in May 2015. In the case of the 2008 breach, preventive actions that it could have taken—and healthcare organizations should consider—included appointing senior leadership with security as their sole focus, security data sharing, end-to-end encryption, tokenization and chip technology, Grogan said.

WHAT HAPPENS TO STOLEN PHI?

At the end of Grogan and Kung's presentation, an attendee asked whether there was a popular use for stolen PHI, and whether it was possible to trace it back to who stole the PHI and who subsequently bought it.

"Healthcare records are so much better than a stolen Social Security number, because a healthcare record has all that information already. You've got Social Security number, you've got financial information and then you have all the medical information about that person, too," Kung said. "You're not just talking about traditional identity theft."

Not to mention that healthcare records can fetch a sizeable amount of money on the black market. While stolen credit card information usually goes for $1 to $2, Kung said, medical records can go for $20 to $50, ranging from pieces of a patient's medical documentation to an entire record.

Chances are slim that an organization will be able to discover who bought stolen PHI. "As for tracking it back, I think that's very difficult to do at this point," Kung said.

Grogan and Kung also fielded a question about what the uses are for knowing someone has a broken leg, for example.

To that, Grogan's only reply was that it's simply a loss of privacy on the part of the patient.—*Kristen Lee*

Analytics, AI Answer Healthcare Data Security Questions

For those unfortunate enough to have experienced a healthcare data breach, they know firsthand that it is a difficult journey full of uncertainty and financial liability, as well as a public relations nightmare. Breaches and hacks have become common news items. The penalties and legal mess that follow a healthcare data breach have frightened many providers into asking themselves the following questions:

- What can be done to avoid becoming yet another data breach victim in this almost-completely digital age?
- What are some of today's products that can improve a healthcare system's security?
- What are some of the innovations available that can outsmart today's cybercriminals?

The increased frequency of medical identity theft is a reminder to organizations of all sizes that healthcare data security threats are real. Many of today's hospitals—including those that have gone through data breaches—use sophisticated and advanced security systems. They use enterprise security software and system management tools that provide in-depth monitoring of hospital systems and capture and store security data in logs. Unfortunately, their systems can still be breached and result in a significant amount of leaked data. The recent UCLA breach is a reminder to everyone that cybercriminals are capable of attacking large organizations and gaining access to millions of patient records.

ANALYTICS MAY BE THE ANSWER

There is more for health systems to consider than just avoiding putting their patients' personal information and financial state at risk. They should still enforce common security standards such as password policies and firewall access controls. Beyond that, security experts recommend looking for answers in the troves of information collected by today's security tools. Some security products gather detailed information on the health of internal systems, remote connection attempts, failed passwords, data transmissions and the behavior of users.

Security firms have begun to apply analytics to this wealth of information to detect anomalies and potential signs that an attack is in progress. It is too complex a task for system administrators to collect and interpret this information without the help of an analytics tool. Security vendors are dangling products with these analytics capabilities to new and existing clients.

Companies such as Dell SecureWorks and Cisco have introduced data analytics into their security products to help customers proactively guard their systems from intruders. On the trail of analytics' entrance into security, it may be time for artificial intelligence (AI) to help with the early detection of a data breach in healthcare. AI is already used to prevent retail theft by monitoring security cameras' live feeds.

HOW TO USE AI FOR SECURITY

AI is capable of evaluating different system logs and traffic patterns within networks, and assessing different events triggered at firewalls or servers. By studying that information, AI can identify abnormalities such as failed passwords attempts or large amounts of data being transferred to servers in different countries.

Security vendors are aware that healthcare is a target for cybercriminals. Whether their goal is stealing and selling patients' personal information or committing insurance fraud to access free health services, hackers will do everything they can to break through firewalls and other security measures to gain access to vulnerable systems. Some hackers are able to stay undetected within systems for months, and leave when they have captured the data they're interested in. Traditional healthcare data security tools may not be sufficient enough to safeguard networks. Adding analytics and AI to the security mix may help prevent and detect future attacks. —*Reda Chouffani*

Wearable Devices and Data: What's Covered—and What Isn't

THE DATA TRACKED and collected by wearable health technology that many people think should be covered by HIPAA may, in fact, not be.

"The things you think are healthcare data may not actually be so," says David Reis, Ph.D., vice president of information services and chief information security officer at Lahey Hospital and Medical Center in Burlington, Mass. "And the things that are healthcare data [under HIPAA] you probably don't expect are."

If someone simply goes to the store and buys a Fitbit, for example, it isn't covered by HIPAA. Therefore, the data collected is not bound by or protected by the regulation.

However, if a person receives a wearable device through their hospital or doctor, the healthcare data that device collects is covered by HIPAA. At least the data that HIPAA defines as protected healthcare information (PHI) is safeguarded.

HEALTHCARE DATA, DEFINED

The best place to start is with the notion that organizations governed by HIPAA are called *covered entities*, Reis says.

"Then within a covered entity, only certain data that covered entity has falls within HIPAA, and the HIPAA Security Rule applies to a subset therein," explains Reis.

While the HIPAA Privacy Rule covers a broader range of information, the HIPAA Security Rule is what hones in on information in electronic format, Reis says.

The HIPAA Security Rule is concerned with PHI and, according to the Human Research Protection Program at the University of California, San Francisco, there are 18 criteria defining what PHI is under HIPAA, including information such as the patient's name, address, phone number and Social Security number (see sidebar, "Healthcare Data Covered by HIPAA," for the full list, page 10).

WEARABLE TECH

HOME

EDITOR'S NOTE

HOW PAST BREACHES CAN INFORM FUTURE DATA SECURITY PLANS

ANALYTICS, AI MAY ANSWER HEALTHCARE DATA SECURITY QUESTIONS

WEARABLE DEVICES AND DATA: WHAT'S COVERED AND WHAT ISN'T

"So *name* is likely a HIPAA-protected data element, but *blood pressure* alone is likely not, unless it is linked to a patient," Reis says. Although a blood pressure reading is something many people associate as sensitive health information, "HIPAA in and of itself generally … is not worried so much about anything other than identifying the patient."

To Reis, that's the key. Blood pressure data or sleep data alone means nothing to hackers if they don't know to whom that data belongs. HIPAA and covered entities are more concerned with protecting personally identifying data and making sure that information, such as a blood pressure reading, isn't and can't be linked to the patient.

A GAP IN HIPAA PROTECTION

Although Reis says he doesn't see many, if any, issues with what HIPAA covers, Kirk Nahra—an attorney at Wiley Rein LLP—takes issue with what HIPAA protects when it comes to health data collected by wearable health technology.

Nahra uses an example involving health and

HEALTHCARE DATA COVERED BY HIPAA

1. Names
2. All geographical subdivisions smaller than a state (street, city, county, precinct and ZIP code)
3. All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date and date of death.
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate and license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web URLs
15. IP address numbers
16. Biometric identifiers (fingerprints, voice prints)
17. Full face photographic images or comparable
18. Any other unique identifying number, characteristic or code

SOURCE: UNIVERSITY OF CALIFORNIA, SAN FRANCISCO auto insurance: If a person is in a car accident, both the health insurer and auto insurer receive that person's medical bills. The health insurer protects that person's health data under HIPAA, while the auto insurer does not.

"That's a weird result," says Nahra, who specializes in privacy and information security litigation as well as a variety of healthcare, insurance fraud and compliance issues. To be fair, Nahra says back in 1996 when lawmakers were drafting HIPAA regulations, they probably weren't thinking about mobile and wearable health technology.

"What's happened in the last, say, decade is we've got more ... situations where health-related information is being created and developed in that gap," he says. And wearable companies not bound by HIPAA fall into that gap.

THE RISKS FROM NONPROTECTED WEARABLES

Noncovered entities can often do whatever they want with someone's data, as long as those potential actions are included in the terms and conditions—which are rarely read by users.

Noncovered entities can often do whatever they want with someone's data, as long as those potential actions are included in the terms and conditions—which are rarely read by users.

A report co-authored by Eric Topol, M.D., professor of genomics at the Scripps Research Institute, found that the U.S. Federal Trade Commission recently tested 12 mHealth and fitness applications and discovered these apps sent consumer data to 76 third-party companies. Furthermore, the report found the shared data included the phone's unique device identifier, the owner's running routes, dietary habits and sleep patterns. A separate report by Privacy Rights Clearinghouse also indicated that 40% of 43 fitness apps collected high-risk data, including addresses, financial information, full name, health information, location and date of birth. The report also found 55% of those 43 apps shared data with third-party analytical services that could potentially link data from the fitness and health apps to other apps that contain identifying information about the user.

The only way data collected by a wearables company like Fitbit would be covered by HIPAA is if Fitbit partnered with a HIPAA-covered entity. Such a partnership is unlikely, according to Reis, because many companies don't want to deal with the complexities of HIPAA.

"I think it would be safe to say that companies like Fitbit would have to think very carefully and have a clear objective on why they would want to enter into agreements with covered entities to store that data because of regulations like HIPAA," Reis says.

In fact, about a year ago at the annual Khosla Ventures CEO Summit, Google co-founders Sergey Brin and Larry Page spoke about this issue. Brin said that because the healthcare industry is so heavily regulated, it's a painful business to be in and not worth it.

"It's just not necessarily how I want to spend my time," Brin said. "I think the regulatory burden in the U.S. is so high that I think it would dissuade a lot of entrepreneurs."

A LAWYER'S PERSPECTIVE

With health data being generated via noncovered entities and HIPAA covering only personally identifiable information from covered entities, Nahra says he sees three possible solutions to fill that gap and ensure better protection of health data:

1. Have a law that regulates the currently unprotected information.
2. Have one law that covers all health information.
3. Completely redefine what is considered healthcare information.

"The third step is sort of an extension of [the second option], which is where you're seeing more and more situations where companies, even in the healthcare industry, are taking information that nobody would think of as health information—like your income or the number of cars you have or your marital status," Nahra says. "[Healthcare providers] are using that to develop modeling on the healthcare side. So if that's true, how do you define what healthcare information is?"—*Kristen Lee*

REDA CHOUFFANI *is vice president of development at Biz Technology Solutions Inc. Follow him on Twitter: @healthcareITGuy.*

KRISTEN LEE *is a news writer for SearchHealthIT. Email her at klee@techtarget.com and follow her on Twitter: @Kristen_Lee_34.*

TechTarget®

Healthcare Data Security Challenges in a Mobile World is a SearchHealthIT.com e-publication.

Scott Wallask | *News Director*

Alex DelVecchio | *Site Editor*

Jacqui Biscobing | *Managing Editor*

Shaun Sutner | *News and Features Writer*

Kristen Lee | *News Writer*

Reda Chouffani | *Contributor*

Linda Koury | *Director of Online Design*

Neva Maniscalco | *Graphic Designer*

Stephanie Corby | *Publisher* | scorby@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER ART: ISTOCK