CONFIDENTIALITY COALITION

GENERAL COMMITTEE MEETING

Thursday, July 26, 2018

3:00 PM to 4:00 PM

Healthcare Leadership Council

750 9th Street, NW, Suite 500 Washington, D.C. 20001

Conference Line: 669-900-6833 or 929-436-2866

Meeting ID: 417 687 1470

1. **Welcome and introductions**
2. **Guest Speakers: Ryan Howells & Dave Lee of Leavitt Partners ATT: 1-2**
3. **OCR Meeting Update**
4. **S. 1850 Update**
5. **Articles ATT: 3-8**

Next meeting: Thursday, September 27, 2018 at 3:00 pm

Guest Speaker Biographies

Ryan Howells

Ryan Howells is a principal based out of the Washington, D.C. office. His work with clients is focused on health insurance market reforms, disruptive distribution channels that have occurred through the emergence of public and private exchanges, and how the implementation of technology can improve the triple aim of reducing costs, increasing quality, and improving outcomes.

Over his career, Ryan has worked in multiple consulting organizations helping national and regional health plans, state and federal government organizations, HIT companies, and delivery systems solve complex problems. Prior to joining Leavitt Partners, Ryan was a vice president and general manager at Connecture, Inc., an industry leader in both public and private exchanges. During his tenure, he managed a multi-million dollar P&L, oversaw 400% growth in less than three years, and was involved in Connecture's IPO in late 2014. He previously spent eight years at iHealth Technologies (now Cotiviti Healthcare) overseeing the implementation of payment integrity and fraud, waste, and abuse solutions for CMS and carriers.

Ryan received his master's in health administration from the University of Southern California where he was a Dean's Merit Scholar and has a bachelor's degree in English from Brigham Young University. He is a Project Management Professional (PMP).

David Lee

David Lee is a director based in Salt Lake City. David provides policy counsel and analysis to clients on issues related to regulations, legislation, and business implications. His work is focused on issues related to government payers, including Medicare and Medicaid, health care reform and other provider issues.

Prior to joining Leavitt Partners, David served as director of Regulatory Affairs and Policy for the National Rural Health Association where he directed advocacy efforts on Capitol Hill and with administrative agencies on issues related to rural hospitals, clinics, health centers, and other providers. Before working at NRHA, David served on the staff of Senator Robert F. Bennett. David received his B.A. at Utah State University in law and constitutional studies while minoring in Spanish. He received his juris doctorate from the Catholic University of America, Columbus School of Law in Washington, D.C.

CARIN Alliance

The CARIN Alliance is a non-partisan, multi-sector alliance co-founded by David Blumenthal, David Brailer, Aneesh Chopra, and former Secretary Mike Leavitt in 2016 to unite industry leaders in advancing consumer-directed exchange. The vision of the organization is to rapidly advance the ability for consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals.

Since 2016, Leavitt Partners has helped facilitate the CARIN Alliance (www.carinalliance.com). Recent work with administration officials has led to Administrator Verma's announcement in March 2018 called the My HealthEData initiative which seeks to provide consumers and their authorized caregivers more transparency into their own health care data using Application Programming Interfaces (APIs).

Among other topics, the alliance is focused on developing industry-wide consensus on the development of a trust framework for how to exchange electronic copies of a consumer's health care data with consumers via third party applications that sit outside of HIPAA leveraging the consumer's individual right of access under HIPAA.

VIEWPOINT

FDA Regulation of Mobile Medical Apps

Jeffrey Shuren, MD, JD
US Food and Drug Administration, Silver Spring, Maryland.

Bakul Patel, MS, MBA
US Food and Drug Administration, Silver Spring, Maryland.

Scott Gottlieb, MD
US Food and Drug Administration, Silver Spring, Maryland.

Mobile apps are increasingly used in health care to promote wellness, treat and diagnose disease, aid clinical decision-making, and manage patient care in hospitals and homes.

Historically, health care has been slow to implement disruptive technology tools that have transformed other areas of commerce and daily life. One factor that has been cited is uncertainty surrounding regulation that accompanies medical products, and how US Food and Drug Administration (FDA) regulations may apply to software platforms. There also are questions in the marketplace about the clinical validity and utility of certain mobile tools.

Efficient regulation can help promote adoption of mobile medical apps. FDA determination that a product developer or manufacturer has met the high regulatory standard for demonstrating clinical benefit and safety (when agency clearance or approval of the app is required) can increase consumer confidence in that technology.[1] In these cases, FDA regulation also can help patients, payers, and investors better understand the performance characteristics of high-quality software products, encouraging a "race to the top" in medical app development.

The FDA position is that efficient regulation of mobile medical apps should be tailored to their potential benefits and risks.

Mobile medical apps may help overcome the siloed, episodic, reactive nature of US health care, whereby patients seek care only after potentially costly health complications occur, and physicians are only reimbursed for expensive in-person office visits that may not reflect the day-to-day reality of the patient experience of living with complex chronic conditions.

Increased demand for mobile medical apps could encourage greater integration of apps with electronic health records (EHRs), potentially allowing clinicians and patients to better manage complex health conditions based on near real-time feedback loops documenting patients' feeling or function. Structured data flows from EHRs and wearable devices could also be used to better inform regulatory decision-making related to drug and device safety or efficacy.

The FDA position is that efficient regulation of mobile medical apps should be tailored to their potential benefits and risks.

After careful consideration, the agency has released guidance[2] that makes it clear that not all these tools are subject to FDA regulation. The agency oversees most mobile apps that are intended to treat, diagnose, cure, mitigate, or prevent disease or other conditions as medical devices under federal statute. Not all mobile apps meet these characteristics. But for devices evaluated, the policies must continue to empower patients and clinicians and facilitate innovation, including by creating regulatory frameworks that give patients and clinicians confidence in the app's performance and reliability.

However, the regulatory framework enacted by Congress in 1976, and incrementally improved since then, is not well suited for software-based technologies, including mobile apps, what FDA and other regulators call "software as a medical device" (SaMD). Congress' regulatory framework was designed for hardware-based technologies. For these devices, developers may only modify products every few months to years, and much can be learned about the technology from its design, composition, and bench testing. The effects of these products on patients tend to be readily observable, and knowledge generated about one product often can be applied to others in the same category to expedite regulatory decision-making. For example, the effect of a synthetic valve replacement device for aortic stenosis on cardiac output can be readily measured and information that becomes known about the performance and failure modes of one such device can be readily applied to the evaluation of a similar synthetic valve.

This regulatory framework uses a risk-based approach to ensure that all devices on the US market provide a reasonable assurance of safety and effectiveness. What a developer must do for its product to meet this standard depends on the risks posed to patients should the device fail to perform as intended. Makers of low-risk devices, such as bandages and eyeglasses, must provide truthful, nonmisleading labeling, implement a system to ensure product and manufacturing quality, report to FDA serious adverse events, deaths, and malfunctions associated with their product, and take appropriate action if and when problems arise.

Makers of moderate- and high-risk devices, such as magnetic resonance imaging scanners and cardiac pacemakers, generally must also gather nonclinical, and sometimes clinical, evidence to show they meet the standard and include it in a premarket submission to FDA for review to determine whether to authorize marketing of the technology. Modifications that could affect the safety or effectiveness of the device undergo a similar premarket review.

By contrast, developers of SaMD, such as clinical decision support software designed to analyze computed tomography results that notifies clinicians of a poten-

Corresponding Author: Jeffrey Shuren, MD, JD, US Food and Drug Administration, 10903 New Hampshire Ave, Silver Spring, MD 20993 (jeff.shuren@fda.hhs.gov).

tial stroke in their patients, can modify their products in response to performance in clinical settings and user feedback every few weeks to months, and little to nothing can be learned about the technology by just reviewing the software code. The influence of apps on patients may be indirect, and knowledge about one software program generally cannot be applied to other programs with the same intended use.

In contrast, SaMD products offer unique opportunities such as addressing malfunctions quickly and efficiently through software updates to minimize adverse events, and directly capturing the effects involving patients outside of the clinical setting, enabling enhanced near-real-time patient engagement and learning. SaMD may also present new challenges, such as addressing cybersecurity vulnerabilities.

The traditional application of FDA's longstanding regulatory framework can stifle the development of, and access to, new and improved SaMD while providing limited patient safeguards. To meet its core mission of promoting and protecting public health, it is important for FDA to create a regulatory framework for SaMD that recognizes the distinctive aspects of digital health technology, including its clinical promise, unique user interface, and compressed commercial cycles for new product introductions and modifications.

To address these challenges as well as the needs of FDA's customers for greater clarity about the agency's regulatory approach, in 2011 FDA began issuing a series of policy guidance[3] to provide market clarity as well as to deregulate many lower-risk functionalities for which active FDA oversight would provide little to no public health value while unnecessarily delaying patient access to potentially beneficial technologies.

These guidance policies addressed those medical device apps for which FDA would continue to actively oversee, called "mobile medical apps," and those that made general wellness claims, and medical device data systems—technologies that receive, transmit, store, and provide simple displays of information—for which the FDA would not[4] require premarket review or notification.

In 2016, in the 21st Century Cures Act Congress amended the Federal Food, Drug, and Cosmetic Act to codify many of these policies and added certain clinical decision support functionalities as no longer being medical devices subject to FDA oversight. The agency also has issued policies to help address cybersecurity vulnerabilities[5] and incidents across the total product life cycle for medical devices, including mobile medical apps.

More recently, FDA has led a working group of regulators from several countries under the auspices of the International Medical Device Regulators Forum (IMDRF)[6] to establish basic policies for a new, pragmatic, and internationally harmonized regulatory framework for SaMD that better meets patients' and clinicians' needs, and the rapid innovation cycles and business models of SaMD developers.

In July 2017, FDA issued a Digital Health Innovation Action Plan[7] that described the actions the agency committed to take to fully implement the software provisions of the Cures Act, including to issue new policy on clinical and patient decision support software, establish a dedicated Digital Health Unit in the FDA's medical device center supported by industry user fee funding, and implement a new regulatory model for digital health technologies consistent with the IMDRF policies.

As part of the latter effort, FDA announced a pilot to create a precertification program under which SaMD developers could be assessed by FDA or an accredited third party for the quality of their software design, testing, and other appropriate capabilities to qualify for a more streamlined premarket review process or in lieu of premarket review depending on the risk of their product while better leveraging postmarket data collection on the device's safety and effectiveness.

This firm-based approach differs from the agency's traditional reliance on individual product reviews. Eligible sponsors could engage in more efficient evidence generation by leveraging clinical data from device registries, EHRs, and other electronic health information sources through the National Evaluation System for health Technology (NEST) that is currently under development. The goal of this program is to collaboratively develop a tailored and pragmatic framework that trusts the excellence of organizations, but continually verifies the safety and effectiveness of SaMD.

Through these innovative approaches, FDA seeks to foster technology innovations. At the same time, the agency is committed to providing consumers and clinicians with better information and greater assurances that medical mobile apps and other digital health medical devices that fall within the agency's regulatory purview are safe and effective.

ARTICLE INFORMATION

Published Online: July 2, 2018.
doi:10.1001/jama.2018.8832

Conflict of Interest Disclosures: All authors have completed and submitted the ICMJE Form for Disclosure of Potential Conflicts of Interest and none were reported.

REFERENCES

1. Statement from FDA Commissioner Scott Gottlieb, M.D., on advancing new digital health policies to encourage innovation, bring efficiency and modernization to regulation. FDA website. https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm587890.htm. Last updated December 17, 2017. Accessed May 22, 2018.

2. Mobile medical applications: guidance for industry and Food and Drug Administration staff. https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf. Published February 9, 2015. Accessed June 27, 2018.

3. Guidances with digital health content. FDA website. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm562577.htm. Last updated March 8, 2018. Accessed June 3, 2018.

4. Digital Health. FDA website. https://www.fda.gov/medicaldevices/digitalhealth/. Last updated May 29, 2018. Accessed June 27, 2018.

5. Cybersecurity. FDA website. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm Last updated April 17, 2018. Accessed May 22, 2018.

6. International Medical Device Regulators Forum (IMDRF). FDA website. https://www.fda.gov/MedicalDevices/InternationalPrograms/IMDRF/default.htm. Last updated April 4, 2018. Accessed May 22, 2018.

7. Digital Health Innovation Action Plan. FDA website. https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf. Published April 26, 2018. Accessed May 22, 2018.

HEALTH AFFAIRS BLOG

To Bring Health Information Privacy Into The 21st Century, Look Beyond HIPAA

Lucia C. Savage

JULY 5, 2018 10.1377/HBLOG20180702.168974

Recently, the *Journal of the American Medical Association* published a "Viewpoint" by I. Glenn Cohen and Michelle M. Mello asking, among other things: "Is HIPAA up to the task of protecting health information in the 21st century?" As federal policy advisers and policy makers have quietly, if insistently, been pointing out since 2014, with the advent of health big dataand social media, the Health Insurance Portability and Accountability Act (HIPAA) alone cannot adequately protect all the privacy and dignitary interests of individuals.

HIPAA was enacted in 1996. A lot has changed over the past 22 years: Today, a person's digital footprints from social media and through their retail spending habits are regularly used to make inferences about health. Even though HIPAA remains "surprisingly functional," significant gaps persist. These gaps, however, derive not from HIPAA per se, but from the patchwork of health information privacy rules outside of HIPAA. The Cohen and Mello "Viewpoint" described one element of this patchwork: the complex rules around and new challenges created by big data analytics. Four additional examples, below, provide a more complete picture of the issues that policy makers need to grapple with, if we are to use health data as effectively as possible while also protecting the people from whom this data comes.

Social Media

In light of the uproar surrounding Cambridge Analytica, Facebook cancelled plans to take HIPAA-regulated health information from hospitals and aggregate it with data from Facebook's social media. But what if Facebook did in fact carry out such a plan? HIPAA does prohibit hospitals from disclosing identifiable health information to any social media company for that company's business purposes. But under current rules, hospitals remain free to contract with a social media company as the hospitals' analytics vendor and business associate to do analysis about the hospitals' population if that analysis is a legitimate health care operation of the hospital. There is some irony in that the nationwide protections from HIPAA apply to how the hospital uses data but do not apply to how the social media company uses data. These differences may no longer serve either consumers or the health needs of the country.

The Role Of States

States have traditionally had wide leeway to enact health and safety laws for the unique needs of their populations. And federal law rarely preempts such laws. In the case of health information privacy, many, if not most, states have done so to protect certain residents from health status discrimination. According to the George Washington University School of Public Health Healthinfo Law database, common examples are for information about mental illness, HIV/AIDS, or reproductive health for girls. Yet, this wide diversity in state law is a barrier to nationwide health information exchange. It also results in confusion by medical professionals and hospitals, consumers, and even lawmakers. HIPAA does not preempt these state laws.

Yet, these laws also mean that we may have less use of this information for learning or improving health. It is well understood that to improve the health of an individual or a population we need to look at data about the whole individual or all aspects of the population. This means having a complete picture of all the factors affecting people's health, from their sexuality to their mental health. But that's not so easy: In the US for example, we have a long and awful history of discrimination against individuals with certain health statuses such as mental illness, HIV/AIDS, sexually transmitted disease, and substance use disorders. To prevent that stigma and discrimination, the majority of state privacy laws allow health information about these statuses to be disclosed only when the individual consents in writing to that disclosure. Of course, this makes it harder to acquire holistic information about people to improve their health. This is compounded by the fact that, because many people fear discrimination, they may be unwilling to consent to the disclosure of certain types of information. And if federal policy makers take us back to the era when people's health status could lead to preexisting exclusions applied to their health insurance, individuals will have all the more reason to not consent to the release of this information. In the age of digital health data, maybe instead of protecting the data from disclosure, we should protect the individuals from discrimination.

Veterans

Another example of health privacy challenges that extend beyond HIPAA is our care for veterans. With our increased awareness of post-traumatic stress disorder in veterans, more than 40,000 homeless veterans each night, and an estimated 20 veterans who commit suicide every day, it might seem that now more than ever we need better, more comprehensive health information about veterans. But, like the state laws discussed above, Title 38 US Code Section 7332 requires that veterans specifically give permission for release of their medical records. This is due in part to the potentially high rates of health status discrimination against veterans for certain medical conditions. Yet, this requirement hampers efforts to consider veterans' overall health needs when developing and evaluating interventions or developing public policies. Some of the tensions raised in both this example and the previous one have also been raised during

a similar debate taking place in Congress right now; members are currently seeking to balance fear of health status discrimination and criminalization of addiction, with the need for comprehensive information about drug use to prevent death.

Following The European Union's Lead

Finally, on May 25, the European Union's (EU's) General Data Protection Regulation (GDPR) went into effect. Among many requirements, this law requires that GDPR-regulated companies (from social media giants such as Facebook and Instagram to smaller businesses that may have a retail web presence in Europe) give individuals copies of their data should they request it from such companies. We already see major corporations such as Microsoft and Facebook extending this EU protection to all customers, including those outside the EU. In the US, health care companies regulated by HIPAA have had a comparable obligation—to give individuals their own health data—since 2000. That now multinational companies beyond the health sphere are extending GDPR to their US customers is a testament to the value for businesses of having a uniform, reliable, predictable set of rules and regulations from which to operate.

As the preceding four examples indicate, the US system for regulating health information, especially outside HIPAA, is certainly not uniform and may not even be predictable. When we think about the task of protecting health information in the 21st century, I do not think it is HIPAA that needs reexamining. Rather, we need an appropriately thoughtful and comprehensive discussion of how best to regulate health information wherever it is collected. If in that discussion we remember human dignity and how we each would want our private information and our health statuses treated, we might just get a result that is more uniform and guards against health status discrimination. Such progress holds the ultimate promise of using data to improve the health of our population and the functioning of the health system.

Why California's New Privacy Law Is a 'Whole New Ballgame'

Attorney Kirk Nahra Analyzes the Strictest Privacy Law in U.S.

Marianne Kolbasuk McGee (HealthInfoSec) • July 9, 2018

While California already had some of the strictest and most varied privacy laws in the country, the new California Consumer Privacy Act of 2018 "is a whole new ballgame," says privacy attorney Kirk Nahra.

The law, AB 375, which was signed by California Gov. Jerry Brown on June 28 and slated to take effect on Jan. 1, 2020, gives consumers the right to ask businesses for the types and categories of personal information being collected.

The law also requires businesses to disclose the purpose for collecting or selling the information, as well as the identity of the third-party organizations receiving the data. Consumers can also request data be deleted and initiate civil action if they believe that an organization has failed to protect their personal data (see *California's New Privacy Law: It's Almost GDPR in the U.S.*).

The new act "is particularly important because it essentially applies to all personal data in all situations," says Nahra of the law firm Wiley Rein in an interview with Information Security Media Group.

"There are some exceptions to that, but the idea is that it applies to everything. And that's very different than all the prior California laws, but [also to] the entire approach to privacy and security regulations that we've seen in the United States to date, where the laws have been either industry specific, like HIPAA [for healthcare] or the Gramm-Leach-Bliley [regulations] for the financial services industry, or they've been practice specific which deals with a particular law for a particular activity," he says.

Until now, "we don't have one size fits all laws, which is why the comparison between the new California law and the European Union's General Data Protection Regulation has been coming up so often lately," he notes.

"This is the first time we've seen this in the United States," he says.

But will it be the last time?

"It's a big question politically whether other states will copy what California is doing under its new privacy law," Nahra says.

In the interview, Nahra also discusses:

- Differences and similarities between the California Consumer Privacy Act of 2018 and the EU's GDPR;
- Who needs to comply with the California law;
- Why there's uncertainty about whether the California law applies to business associates under HIPAA.

As a partner at the law firm Wiley Rein LLP, Nahra specializes in privacy and information security issues, as well as other healthcare, insurance fraud and compliance issues. He's a member of the board of directors of the International Association of Privacy Professionals and was co-chair of the Confidentiality, Privacy and Security Workgroup, a former panel of government and private-sector privacy and security experts advising the American Health Information Community.

Amazon's Healthcare Push Could Run into HIPAA Compliance Issues

Amazon has been expanding rapidly into the healthcare field, but its approach to patient privacy could use a lot of tweaking if the company doesn't want to run into HIPAA compliance problems down the road.

HealthIT Security

By Fred Donovan

July 09, 2018 - Amazon has been expanding rapidly into the healthcare field, but its approach to patient privacy could use a lot of tweaking if the company doesn't want to run into HIPAA compliance problems down the road.

Amazon has set up a health and wellness team within its Alexa division to make the digital voice assistant more useful in the healthcare field.

The company has also joined with Berkshire Hathaway and JP Morgan to form a joint healthcare company to provide healthcare to their employees, and it recently purchased home delivery pharmacy company PillPack for around $1 billion.

Dig Deeper

- Amazon's Alexa Healthcare Team Bones Up on HIPAA Compliance
- Amazon HIPAA Compliance Lead Search Indicates Healthcare Focus
- How to Create Efficient, Compliant Healthcare Virtualization

But the company recently demonstrated a cavalier approach to a breach of patient privacy that doesn't bode well for its ability to protect medical information and respond to health data breaches.

Vernon, Connecticut resident Leah Luce recently purchased a medical alert bracelet from a third- party seller on Amazon.com. The bracelet included Luce's name, date of

birth, emergency contact information, and medical condition printed on the inside of the bracelet, explained a report by NBC Connecticut.

Luce was then informed by her physician that photos of her bracelet with her medical information were visible on the Amazon website in advertisements for medical ID bracelets, the report noted. Luce called Amazon and an agent told her the company would investigate. She later received an email from Amazon saying that the company could not release the outcome of the investigation.

Obviously, this part of Amazon has not been trained on how to handle patient privacy breaches. As Amazon continues its healthcare expansion, it will need to do a lot better job of putting medical data security policies in place and training employees on how to handle breaches.

Luce ultimately got satisfaction when she contacted NBC Connecticut. The TV station sent emails to the seller of the bracelet, Personalized Love Jewelry, which responded almost immediately with an apology and a pledge to remedy the situation.

"All Marketplace sellers are required to follow our selling guidelines and those who do not will be subject to action, including potential removal of their account. The products in question are no longer available," Amazon said in its response to NBC Connecticut.

The TV station confirmed that the photos of the bracelet with Luce's medical information is no longer available on the Amazon site.

Sellers like Personalized Love Jewelry fall into a gray area when it comes to HIPAA. They occasionally handle PHI but they are not considered a covered entity or a business associate under HIPAA.

According to HHS, a covered entity is a healthcare provider, a health plan, or a healthcare clearinghouse. A business associate is a "person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity."

Mobile health apps also fall into this gray area. The American Hospital Association (AHA) recently warned about the potential misunderstanding among consumers concerning mobile health apps and HIPAA.

"Commercial app companies generally are not HIPAA-covered entities. Therefore, when information flows from a hospital's information system to an app, it likely no longer will be protected by HIPAA," AHA noted in its comments on the CMS hospital inpatient prospective payment system proposed rule for fiscal year 2019.

"Most individuals will not be aware of this change and may be surprised when commercial app companies share their sensitive health information obtained from a hospital, such as diagnoses, medications or test results, in ways that are not allowed by HIPAA," AHA noted.

Providers of medical alert bracelets would likely fall into a similar category as commercial app companies when it comes to HIPAA. In the case of Luce, neither Amazon nor the bracelet seller was not subject to HIPAA rules, but the tech giant is getting into business areas in which HIPAA will come directly into play.

Amazon will need to do a better job at handling patient privacy complaints regardless of what area of the business is dealing with the aggrieved customer. If not, Amazon will be facing increasing consumer distrust and potential regulatory scrutiny.

The Cybersecurity 202: Big tech is going after California's new privacy law

By Derek Hawkins July 3

The Washington Post

THE KEY

Big tech is going after California's new privacy law in an attempt to weaken it before it takes effect in 2020.

Tech industry lobbyists representing giants like Google, Uber, Amazon and Facebook are pushing for changes to the recently passed California Consumer Privacy Act, which contains the country's strongest data privacy protections and could significantly change the way they do business. The tech giants are worried that the new law could hamper their operations and herald tougher regulation on the national level in the wake of controversy over how these companies share users' data.

Industry groups lobbying for changes haven't said specifically what they want to see modified, but they're making clear they intend to play a major role in negotiations over the coming months. They include the Internet Association -- which represents Google, Amazon and other tech giants, as well as TechNet and the Interactive Advertising Bureau. (Amazon CEO Jeffrey P. Bezos owns The Washington Post).

"It is going to take time to fully understand the implications of this bill for California's consumers and economy," said Robert Callahan, vice president of state government affairs for the Internet Association. **"The bill was written in a hurried and ill-considered process, and received very little input from those affected by the legislation. Changes will be necessary as businesses of all types look at implementation."**

The law, signed by the governor late last week, requires tech companies to disclose the type of data they collect on customers and reveal the advertisers and other third parties they share it with. It also gives users the ability to opt out of data collection and empowers the state attorney general to punish companies that don't protect user information.

Legislators introduced, debated and passed the law in the span of less than a week to head off a ballot initiative that contained even tougher privacy protections, as my colleague Tony Romm has reported. The initiative's main backer agreed to withdraw his proposal if lawmakers passed a compromise bill before a June 28 deadline to get the measure on California's November ballot.

Google, Uber and other giants fought to kill Alastair Mactaggart's initiative, which drew more than double the signatures needed to be put to a vote, Tony reported. But they ultimately came to accept the compromise legislation — likely because it's easier to change than a ballot initiative, according to Ashkan Soltani, an independent researcher and technologist who helped craft the measure .

"Part of the calculation by industry was to try to move Mr. Mactaggart off the table to bring this back into a standard legislative lobbying process," Soltani told me.

"Moving forward, I think we will make clarifications, but the goals of the bill won't change," State Sen. Bob Hertzberg (D), who co-authored the legislation, said in an emailed statement. "The value of keeping these discussions in the Legislature is that as technology evolves, we will be able to have thoughtful conversations about how to balance innovation with the ability of consumers to control their private information, know if it's being sold, and delete it if necessary."

The law's January 2020 implementation date gives critics ample opportunity to amend it.

Google, in comments to the Hill newspaper, said that "we look forward to improvements to address the many unintended consequences of the law." The Interactive Advertising Bureau, a digital advertising trade group whose members include Facebook and Microsoft, said it too was weighing its options. "This is the broadest, [most] sweeping piece of privacy legislation in the nation now, without question, so we are doing our due diligence as to what it means," Brad Weltman, the organization's vice president of public policy, told the Wall Street Journal.

The law also has detractors on the consumer side. The American Civil Liberties Union of Northern California said the law "fails to provide the privacy protections the public has demanded and deserved" in the wake of the Cambridge Analytica scandal and other high-profile cases of data misuse. "This measure was hastily drafted and needs to be fixed," said Nicole Ozer, the group's technology and civil liberties director.

Despite those criticisms, the measure is already being held up as a bellwether for privacy initiative in other states and nationally. Soltani said that's important for Big Tech to keep in mind as they work to influence the final version. "If the measure is weakened too substantially," he said, "the industry risks having an even worse intervention than what's on the table now."

Healthcare Organizations Must Strengthen Their Cybersecurity Immunity To Avoid Falling Victim To Cybercriminals

Information Security Buzz
By Nikolai Vargas
July 2, 2018

Cybercriminals looking to make a profit are turning their attention towards an industry known for housing sensitive consumer data with weak security protocols: healthcare.

In April of 2018, Utah-based company HealthEquity reported 23,000 accounts were compromised in a data breach when an employee fell for a phishing scheme. As a result of human error, information like employee names, deduction amounts and social security numbers were exposed.

The HealthEquity breach is hardly an isolated incident in healthcare. A former employee, for example, was caught inappropriately accessing the medical records of 29,000 patients at SSM Health in St. Louis, Missouri. In Chicago, two of Sinai Health Systems employee email accounts were caught in a phishing scam, impacting the records of 11,350 patients. 2017 alone saw the U.S. Department of Health and Human Services report an approximate 477 healthcare breaches and the exposure of more than five million patient records.

While organizations can't control the actions of cybercriminals and rogue staff members, they can address how employees approach security and mitigate the risk of a breach by strengthening internal cybersecurity habits.

Healthcare providers are feeling the impact of putting off cybersecurity for years

Historically, healthcare organizations have neglected cybersecurity best practices in order to focus on what they do best: providing excellent patient care. But this has left employees wholly unprepared to deal with cyber threats when they inevitably occur.

Given the sheer volume of breaches caused by human error, it's no surprise to learn that 80 percent of health IT professionals are concerned about employee security awareness. Employees are the weakest link within an organization — more often than not, breaches are the result of human error because someone didn't comply with or understand security best practices. Today, employee mistakes account for more than one third of 'threat actions' hurting the healthcare industry.

Seemingly innocuous activities, like sending sensitive files over email instead of a secure intranet, can actually help hackers bypass the even the strongest security measures. Similarly, connecting unauthorized applications to healthcare networks pokes holes in existing defense mechanisms. That popular messenger app everyone's been talking about? If employees use it on a hospital's network, it could be putting internal servers and sensitive information at risk. A recent Igloo Software survey found 30 percent of healthcare employees will use apps that provide the greatest convenience over ones that have been approved by their employer's IT team.

Education is the key to eliminating risk brought on by human error

Healthcare organizations continue to struggle to provide sufficient awareness training to their internal teams, making it difficult for employees to strengthen their security hygiene. And IT professionals agree the lack of education is taking a toll on their organization's ability to respond to threats. A recent study conducted by the Ponemon Institute revealed 52 percent of American healthcare executives believe the lack of security awareness impacts their security posture.

The need for security education is so important that regular training is now a requirement to demonstrate compliance with Health Insurance Portability and Accountability Act (HIPAA) Rules. Because cyber attacks are evolving every day, effective awareness programs need to provide regular training to employees whenever threat intelligence is shared. Ideally, cybersecurity updates should be given monthly while security training should be provided a couple of times per year.

Within the training program, employees should learn how to distinguish between different threats and have the opportunity to act out their response in simulated environments. A routine phishing test, for example, evaluates an employee's ability to distinguish between a real and a fake email. Quarterly reminders about the dangers of phishing and easily accessible learning materials can also help workers keep cybersecurity top of mind. In addition to training sessions and skills tests, healthcare providers can encourage security best practices by:

- Incorporating cybersecurity education in new employee onboarding materials.
- Administering routine phishing tests and regularly assessing employees' security knowledge.
- Notifying teams when new threats emerge with real examples and ways to respond.

Organizations can't afford to ignore the state of their cybersecurity, not when there's personally identifiable information (PII) at stake. In order to successfully tackle online threats, healthcare providers will need to empower their employees to be a robust first line of defense against impending cyber attacks.

Augment employee training with robust tools for total security coverage

To create a truly holistic cybersecurity environment, organizations should supplement awareness training with security tools monitoring networks and devices around the clock. Securing a healthcare environment requires a multi-pronged approach — layered defenses, not one

dimensional strategies, will ensure PII and other sensitive information remain safe from criminals.

One common best practice organizations are using is requiring employees to enable multi-factor authentication (MFA) when connecting to workspace and company accounts. By adding an extra layer of security, such as a code sent via text message or fingerprints, MFA ensures stolen login credentials can't be used to infiltrate internal systems. As employees bring their personal devices into work, healthcare organizations can deploy a bring your own device (BYOD) policy, clearly articulating what files and servers workers can connect to on their mobile device.

In addition to strengthening account security and policing mobile devices, healthcare providers can leverage tools like antivirus software and content filtering solutions to protect healthcare environments. Firewalls, analytics and machine learning tools also help hospitals detect threats in real-time and stop hackers in their tracks. Implementing an identity access management (IAM) solution enables organizations to monitor employee access to PII and immediately restrict access to information when authorized users are detected. Regularly auditing healthcare networks for vulnerabilities also allows healthcare organizations to test their cyber resiliency and make adjustments when necessary.

With proper awareness training, employees are less likely to fall for spam emails and avoid creating vulnerabilities that hackers are waiting to exploit. Using a combination of education and security software, healthcare organizations can minimize the human element risk and strengthen their overall security posture. By empowering employees with the tools to address cyber threats head on, healthcare organizations can stay a step ahead of criminals and shut down a breach before it even takes place.