Health Information Compliance Alert

Enforcement News: Pay Attention To Risky BYOD Trends

Plus: Your mobile health app could be the weak link in your security chain.

The emerging trend of employees using their own mobile devices for work purposes has extended to the healthcare industry in the past few years, and this trend has raised some serious HIPAA concerns.

In fact, the Bring Your Own Device (BYOD) movement is inciting employers to increasingly develop and institute specific policies. One of the major trends for 2016 is the BYOD will become the norm, observed Rochester, N.Y.-based attorney **Joseph Carello** in a Jan. 14 blog post for **Nixon Peabody LLP**.

"The U.S. workforce is becoming increasingly mobile, and this mobility will require employers to permit employees to use personal mobile devices with which employees are most comfortable and productive," Carello noted. "This continued shift to BYOD will strain IT and privacy professionals who seek to maintain the integrity of confidential business, consumer and employee information."

What's more: And an inevitable byproduct of the BYOD trend will be an increase in litigation regarding BYOD use, Carello said. Also, a continued rise of wearables like "smartwatches" will create a struggle for healthcare employers to keep track of where sensitive data resides.

Beware: Your Mobile Health App Isn't Secure Enough

If your practice uses or provides patients with a mobile health application, you should know that your app is most likely fraught with serious security risks that the app developer has not addressed.

So says **Arxan Technologies**' 5th Annual State of Application Security Report Healthcare Edition, which examined 71 popular mobile health apps, 19 of which were approved by the **U.S. Food and Drug Administration** (FDA). Arxan focused the report on cyberattacks happening at the application layer.

Among the 71 popular mobile health apps, 86 percent had at least two risks ranking in the Open Web Application Security Project's (OWASP) top 10 risks. For instance, 97 percent of the apps lacked binary protection, 79 percent had insufficient transport layer protection, and 56 percent had unintended data leakage.

More than half of consumers who use mobile health apps, as well as nearly half of executive IT decision makers, expect their health apps to be hacked within the next six months, the report said. And 76 percent of health app users said they would change providers if they knew the apps they were using were not secure, while 80 percent said they would change providers if a similar provider offered an app that was more secure.

Link: To read the report, go to www.arxan.com/wp-content/uploads/2016/01/State_of_Application_Security_2016_Healthcare_Report.pdf.

Are You Ready For 2016's HIPAA Audits?

As expected, HIPAA audits will continue this year and they will expand to more entities. If you haven't already, now is the time to prepare your organization for a visit from the **HHS Office for Civil Rights** (OCR).

Starting early this year, OCR will begin performing random desk and on-site audits of not only covered entities (CEs), but also business associates (BAs), according to a Jan. 28 alert by attorneys **James Bailey** and **Kelsey Farbotko** of the law firm **Williams Mullen**. "These audits are expected to focus on areas of noncompliance that OCR has witnessed in its previous audits and enforcement actions, such as risk analyses and use of encryption technology."

Best practices: Before undergoing an OCR audit, make sure that you're complying with the HIPAA Privacy, Security and Breach Notification rules. At a minimum, ensure that your organization:

- Has documentation of and compliance with privacy and security policies and procedures;
- Performs security risk analyses of electronic protected health information (ePHI);
- Uses Business Associate Agreements (BAAs) appropriately;
- Disseminates a Notice of Privacy Practices (NPP) as required;
- Documents any and all breaches in accordance with HIPAA; and
- Has systems and protocols in place to properly address a breach.

"With HIPAA audits right around the corner, healthcare practitioners, providers and their [BAs] need to place additional focus on carefully evaluating their past and current HIPAA compliance to identify and strengthen any areas of potential noncompliance," Bailey and Farbotko urged.

Large-Breach Count Down For January 2016

The number of breaches affecting more than 500 individuals reported in January 2016 paled in comparison to December 2015's whopping 23 breaches. In the first month of the New Year, there were only nine reported large breaches.

And healthcare providers reported six of those breaches, while health plans reported three, according to the **HHS Office for Civil Rights** (OCR) "Wall of Shame" (https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf), which displays all reported large breaches affecting more than 500 individuals.

Unauthorized access/disclosure accounted for most of the January breaches (four), while hacking/IT incidents accounted for two breaches, and theft, loss and improper disposal each accounted for one breach. Five breaches involved paper/films, while one breach each involved email, a desktop computer, a laptop and a network server.

The two largest breaches in January both involved health plans. **New West Health Services** (d/b/a **New West Medicare**) in Montana reported a breach affecting 28,209 individuals, caused by loss of a laptop. **Blue Shield of California** reported a breach affecting 20,764 individuals, caused by unauthorized access/disclosure involving a network server.

Don't Miss The Deadline For Reporting Small HIPAA Breaches

If your organization experienced one or more breaches involving fewer than 500 individuals during 2015, the deadline for reporting those breaches to the **U.S. Department of Health and Human Services** (HHS) is approaching fast.

You must report such "small" breaches to HHS by Monday, Feb. 29, 2016 — under the HIPAA regulations, small breach reporting must occur within 60 days of the end of the calendar year. And if you miss this deadline, you could face "separate and distinct penalties" for failing to report a HIPAA breach in a timely manner, according to a recent alert by attorneys **Bruce Armon** and **Karilynn Bayus** of the law firm **Saul Ewing LLP**.

If your organization is a covered entity (CE) that delegates its breach-reporting responsibilities to a business associate (BA), you should confirm that the BA files the report in a timely manner, Armon and Bayus advised. "The best practice would be for the CE to review the breach report before it is filed with HHS to ensure that it is accurate."

To report your small 2015 breaches to HHS, go to www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.

How Your 'Meaningful Use' Obligations Will Change Drastically

The **Centers for Medicare & Medicaid Services** (CMS) is planning to effectively end the Medicare Electronic Health Record (EHR) Incentive Program, also known as Meaningful Use.

CMS is using legislative flexibility under the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) to shift the Medicare EHR Incentive Program towards a new set of goals, according to a Jan. 19 blog posting by CMS Acting Administrator **Andy Slavitt** and HHS Acting Assistant Secretary for Health **Karen DeSalvo**. The new goals are to:

1. Reward providers for the outcomes technology helps them to achieve with their patients;
2. Allow providers the flexibility to customize health IT to their individual practice needs;
3. Level the technology playing field to promote innovation, including for start-ups and new entrants, by unlocking electronic health information through open application program interfaces;
4. Prioritize interoperability by implementing federally recognized, national interoperability standards and focusing on real-world uses of technology.

The blog posting came on the heels of Slavitt's Jan. 11 speech at the J.P. Morgan Annual Health Care Conference, in which he announced: "The Meaningful Use program as it has existed will now be effectively over and replaced with something better."

As CMS works through this transition to the new program, keep in mind that you will still be subject to the Meaningful Use program's existing requirements and standards, including those for Stage 3. "While MACRA provides an opportunity to adjust payment incentives associated with EHR incentives in concert with the principles we outlined here, it does not eliminate, nor will it instantly eliminate all the tensions of the current system," Slavitt and DeSalvo wrote.

Also, MACRA addresses only Medicare physician and clinician payment adjustments and doesn't include Medicaid, so the EHR incentive programs for Medicaid and Medicare hospitals have different sets of statutory requirements. Finally, CMS is moving forward with new authority to streamline the process for granting hardship exceptions under Meaningful Use, allowing groups of healthcare providers to apply for an exception instead of each physician applying individually.

Resources: To read a transcription of Slavitt's Jan. 11 speech, go to https://blog.cms.gov/2016/01/12/comments-of-cms-acting-administrator-andy-slavitt-at-the-j-p-morgan-annual-health-care-conference-jan-11-2016/. You can access the CMS blog posting at https://blog.cms.gov/2016/01/19/ehr-incentive-programs-where-we-go-next/.