ISSUE
19
AUTUMN
2018

THE
NORTHWEST'S
HIPAA SECURITY
BULLETIN

HIPAA SAFE

CONTENTS

Wearable Health Technology – ePHI?

Consumer based wearable health technology use continues to increase, even as electronic protected health information (ePHI) breaches also climb. More people are monitoring their steps taken per day, their heart rate or other information associated with individual health. But is a Fitbit (for example) storing HIPAA-protected ePHI?

The short answer is probably not. HIPAA governs Covered Entities (CE) and Business Associates (BA), and not individual people collecting their own information. Likewise, if an employer offers wearable health technology as part of a human resources incentive program, then HIPAA still does not apply – even if the employer is a CE or BA. Two examples where this data becomes ePHI and is protected under HIPAA:

- an employer links wearable information to a healthcare organization (e.g. provides data for treatment or uploads data into an electronic health record, etc.)
- a physician provides a patient with wearable technology to manage healthcare.

Many wearable manufacturers have built reasonable security controls into their products, but we encourage our readers to practice protecting their own health information - regardless of vendor claims.

It's 2018 and Phishing is a BIG Deal

It seems that every week this year includes a news article detailing how ePHI was stolen through criminal phishing activity. In the summer of 2016 we included a back-page article explaining phishing, provided some free workforce training resources and demonstrated how a compliance officer or HIPAA security officer can reference Security Rule citations to justify the expense of a phishing campaign (Issue 10). In the two years since, criminals have advanced their techniques and leveraged phishing related malicious software (i.e. malware) to a much darker purpose that moves from stealing credit cards and personal information to encrypting electronic health record (EHR) systems. Encryption uses a math algorithm to change electronic information (e.g. ePHI) and render it unreadable to anyone lacking the encryption key. Once encrypted, criminals demand payment to decrypt the ePHI and healthcare entities either quietly pay for access to their ePHI or try to restore their EHR from backup media. The encryption and payment attack is more broadly described as "ransomware". Either ePHI recovery approach removes the EHR from clinical staff and directly affects patient care.

Compounding the issue, criminals are now also establishing ransomware-as-a-service models, which partner with malware programmers to share profits gained from healthcare organization payments. These services are fully modern, accept cryptocurrency (a type of electronic payment) and make it difficult for law enforcement to trace any transaction.

The Office of Civil Rights has made it clear that **any CE or BA that has experienced a successful ransomware attack has a reportable breach event**. We may be going out on a limb to say this, but we believe that phishing is one of the most impactful and expensive attack vectors in (at least) the healthcare industry and all organizations should perform phishing campaigns quarterly if possible. Please contact us if we can help facilitate a phishing project for your company.

PROTEUS
CONSULTING
www.ProteusID.com

Inactive Workforce AD Accounts

We are asked periodically what to do with ex-workforce members' Microsoft Active Directory accounts. Complicating this issue in healthcare is that some people purposely float in and out of a hospital or practice (e.g. medical students, per diem nurses, etc.). The HIPAA Security Rule requires unique user identification and we do not recommend using generic accounts to manage transient employees. We recently discussed this issue with a group of security workers across various industries who recommend:

- timely disabling inactive accounts upon a person's routine departure
- expediting account inactivation for fired or other abnormal reasons for departure
- isolating inactive accounts in a named organizational unit container
- replacing the account's password with a LONG random passphrase text
- removing account associations (e.g. group memberships, etc.)
- closing linked accounts (e.g. applications, cloud-based services, etc.)
- adding a (Julian calendar) date text to the user name, to increase its attention (e.g. if the account was lingering in a list or group account)
- archiving account specific files to avoid "orphaned" information not related with a user account, and
- documenting actions and processes, in the event that a terminated account needs to be re-created.

There is no one solution that is perfect for every AD environment. Sorting and managing accounts will reduce the risk of an ePHI unauthorized disclosure event and of co-workers using another's credentials. Ultimately, an AD user account management risk evaluation should drive a discussion and reveal appropriate solutions to archive accounts that otherwise could be deleted. **Additional ePHI access termination tips can be found in Issue 16.**

Company News

We are taking a break from reserving 100% of our newsletter for HIPAA Security and like-industry news to remind you that we're consistently working to provide our customers more value. What started as an ePHI risk analysis-based company grew into developing superior policies and procedures, then offering various training avenues. We are proud to now include "Virtual Compliance" (e.g. reducing your risk register action items, etc.). As HIPAA Security remains our sole discipline, we don't (directly) provide traditional IT security services – although we work closely with companies that we trust to deliver HIPAA-quality 164.308(a)(8) technical testing, etc. *Please check out our website* (www.ProteusID.com) for more information and give us a call or email if we can help. As a reminder, PROTEUS offers:

HIPAA based risk and compliance analyses
HIPAA Security Rule policies and procedures
HIPAA Security Rule based training
HIPAA Security compliance support

> ***"Since opening our company in 2012, our primary goal remains to offer products and services that are identified through working with our client-partners." – Proteus Consulting***

The Value of Walking Spaces

Some of the best HIPAA Security programs we've seen include a hands-on compliance or security officer regularly observing how well people and spaces (e.g. offices, hallways, patient waiting areas, etc.) protect PHI from unauthorized disclosure.

Different from the risk analysis, showing up and speaking with workforce members more supports a compliance assessment. One strategy is to ask the facilities team or office manager to walk each space on a rotational basis with a checklist (some of our customers do this exact thing) and observe whether appropriate doors are locked, laptops (and paper records) are secured, etc. A second approach is to generate a question or three for every calendar month and then randomly canvass co-workers to gauge their understanding of key program pieces (e.g. who the HIPAA security and privacy officer are, where security incidents are reported, etc.). Something to add to any methodology is to confirm and report workstation inventory (e.g. computers, laptops, tablets, medical devices, etc.) for the location being walked.

ARTICLES BY ALAN DAVIS
PROTEUS CONSULTING
HAYDEN, ID 83835
(208) 215.5607