ISSUE
16
WINTER
2017

THE
NORTHWEST'S
HIPAA SECURITY
BULLETIN

HIPAA SAFE

CONTENTS

WPA2 Wireless Protocol Broken

WPA2, the current wireless encryption standard, was compromised mid-October using a new method named KRACK (Key Reinstallation AttaCK). If exploited, KRACK can potentially allow a criminal to either view information being shared or access unsecured wireless devices on the same network. Here are some precautions that you can take to reduce your risk:

- use additional security protocols. HTTPS, TLS or IPSec can provide an additional layer of security that keeps network traffic packets encrypted
- consider not broadcasting your wireless SSIDs. One of our hospital customers has been doing hiding their SSIDs as a security control for years and has no problems providing wireless connectivity to approved devices.
- patch all wireless device and access points when available. Don't' forget about any Internet of Things (IoT) devices, including medical equipment
- consider limiting Wi-Fi access

This is BIG news from the cryptography community. The race between secure communications and hackers does not start or finish with this latest exploit. With education and additional security measures intelligently applied, your team can keep calm and continue to protect their patients' ePHI.

Terminating ePHI Access

How thoroughly does your organization manage addressable implementation specification "Termination Procedures" §164.308(a)(3)(ii)(C)? Our experience is that most Covered Entities (CE) have some kind of communications between Human Resources (HR) and Information Services (IS), but that the process leaves some residual risk to the company.

Termination procedures should entail a consistent process where all access is discontinued and affected team members should be aware of the processes outside of their immediate responsibility (e.g. HR should be notified when keys are turned in, etc.). Aside from deleting all network and system login credentials, we recommend **terminating physical facility access** by collecting physical keys, changing electronic security codes, updating access lists, and collecting identification cards or badges.

One area we often see overlooked is electronic protected health information (ePHI) stored on personal devices, including cell phones and laptops. Even if a company has an administrative policy forbidding ePHI being shared in email, we don't consider this an adequate security control and **assume that ePHI is on a personal device until proven otherwise**. The IS team should develop processes to **wipe all organization accounts and data** from the device, such that no ePHI leaves with a workforce member.

The termination process applies to anyone with potential access to ePHI. Don't forget to **develop processes to manage contractors, Business Associates (BA) and other vendor access**. Communicate regularly with each external company with ePHI access; remove their inactive employee accounts and ensure that no new employee is using their predecessor's credentials.

It is very important to develop a repeatable and manageable process to protect ePHI when a workforce member leaves the organization. Unauthorized ePHI access by a former employee has been the cause of many reported breaches. Ensure that your organization addresses this important HIPAA citation.

PROTEUS
CONSULTING
www.ProteusID.com

Limiting Whistleblower Risk

Consider that you just thoroughly completed your termination process for an employee walking out of your building. Are you equally confident that this person leaving isn't planning to accuse the organization of unlawful conduct? While not part of the HIPAA Security Rule, HIPAA does allow a "whistleblower" to either call the Office of Civil Rights (OCR) or disclose patient information to a private lawyer as part of a qui tam lawsuit. In the case of an OCR phone call, the ex-employee can maintain anonymity. While these two reasons should not drive a compliance program or compel a CE (or BA) to apply reasonable and appropriate security controls to protect ePHI, the potential for financial damages from not properly resourcing a HIPAA Security (or Privacy) program are real. Notably, the idea of bringing PHI to a lawyer seems to be in direct conflict with the rest of the HIPAA laws, which are meant to keep PHI private.

We recommend including whistleblower education as part of a CE or BA HIPAA training curriculum. This advice may seem counter-intuitive, but we believe that training isn't going to motivate an ex-employee to act and that it is better to not risk additional liability through improper disclosure (e.g. by the ex-employee reporting the incident or exposing PHI to a local news station, etc.). Additionally, your workforce may use the training opportunity to address concerns and improve communications or correct an unsafe situation.

The absolute best way to limit the risk of a whistleblower action is to mature and implement policy, procedures and processes that address each applicable HIPAA Security, Breach Notification and Privacy citation. Self-assessments, using the 2016 OCR Audit Protocol, are an excellent way to identify gaps and protect (e)PHI.

More Mobile Workforce Security Tips

Secure Your Workforce

- Train employees that malware can affect any common computing device
- Train employees to understand mobile device vulnerabilities and risks
- Perform in-house phishing tests and identify weaknesses
- Don't forget about periodic security reminders

Secure Your Devices

- Require malware detection software on any trusted endpoint (phones, tablets, etc.)
- Ensure that ePHI applications and network sessions terminate after a period of inactivity
- Require authentication (e.g. a six-digit PIN) to unlock a device
- Require all devices install applicable security patches
- Require encryption for data at rest
- "Sandbox" sensitive information

Secure Your Connections

- Require strong encryption for data in transit
- Don't use unsecured Wi-Fi networks
- Use virtual private networks to connect to the corporate network

"Compliance is about applying steady effort to your program. HIPAA isn't a 'once and done' business."

ePHI Security Responsibilities

Health and Human Services recently sent a reminder for CE and BA to help understand their requirements to protect ePHI. The notice detailed:

- Being aware of the obligations of the HIPAA Rules and how they apply to business operations. 45CFR sections 160 and 164 should be known by your HIPAA Security team members, as should present day trends (e.g. phishing is a very popular and current attack method)
- Creating formal plans to respond to security incidents and contingencies that may make ePHI unavailable. Don't forget to test your policies and procedures prior to an event
- Respond to security incidents (and violations of policy and procedure that endanger ePHI). We see many organizations that handle incidents "ad hoc" without any consistent means or feedback to the HIPAA Security Officer
- The requirement to report unauthorized disclosure (i.e. Breach) events. Those events affecting 500 or more patients must be reported to the OCR and to the media within 60 days, unless law enforcement requests a delay. Events affecting less than 500 people are also required to be reported to OCR within 60 days of the next calendar year. Do not include any ePHI in the report submission. Reference §164.400 series for a complete description of the HIPAA breach reporting requirements.

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