ISSUE
17
SPRING
2018

THE NORTHWEST'S HIPAA SECURITY BULLETIN

HIPAA SAFE

CONTENTS

Meltdown and Spectre

The Department of Health and Human Services issued a severity level 2 (Medium) technical report in January that detailed a pair of recently discovered computing processor chip vulnerabilities that could affect computers, including healthcare workstations and medical equipment. The affected processors are potentially susceptible because they don't always check JavaScript programming code. Criminals can engineer JavaScript instructions to fool a computer processor into disclosing information entered into a web browser application (manually or via an automated means). This information can include user names and passwords, session cookies, or electronically protected health information (ePHI).

Meltdown and Spectre affect different processor platforms and luckily, the Spectre vulnerability is pretty difficult to exploit. We recommend contacting medical equipment companies to learn which of your devices are vulnerable and what security update patches are available if a device is at risk.

Many service providers and web browser applications have already patched their services to prevent these two vulnerabilities from being realized. We still recommend checking that all medical devices are protected against exploitation.

"Cloud" (Remote) Data Centers and HIPAA

For many reasons, including reducing risk, a number of Covered Entities (CE) are turning to regional medical application and database service companies to host their electronic health records (EHR). A Business Associate (BA) relationship is borne in these cases and both parties need to clearly communicate the details of their HIPAA compliance programs to ensure that ePHI is appropriately protected. We're seeing a trend of CE trusting the BA's security controls without knowing whether these **controls align with the CE policy and procedures** documents or **whether the controls are even reasonably secure**. Here are **some** details to consider if a CE has moved to a cloud-based EHR:

- is the CE aware of the EHR system's password parameters? What are the passwords' length, complexity and change frequency? Is the system configured to remember and not allow previously used passwords?
- does the BA monitor your organization's EHR login attempts? What reporting does your BA provide the CE supporting failed login attempts and how often is this report provided?
- how are inappropriate ePHI access audits performed? What information is exchanged between the CE and BA, and how often?
- what is the BA's backup plan and how often are backups tested? Are failover redundant data stores used in the place of backup media? Is there an alternate data site where EHR information is duplicated in the event of a primary location emergency?
- how does the BA define a security incident and what involvement or reporting is required to the CE in the event of an incident?

Using a cloud provider to host an EHR can save a CE money and improve ePHI availability. But the CE must continue to lead the work that documents and ensures the security controls in place to reduce risk. Both the CE and BA need to understand what the other is doing or is expected to do to protect their ePHI, to promote a compliant HIPAA program.

PROTEUS
CONSULTING
www.ProteusID.com

Access to ePHI Security

To compliment last issue's ePHI access termination article, we think it beneficial to discuss approaches to granting ePHI access. The first thing a CE or BA must do is **implement policies and procedures to ensure that all workforce members have appropriate ePHI access**. This means providing your workforce with intentions, and assigning responsibilities to specific positions to create local processes that provide consistent ePHI access to those that require such, and to prevent workforce members who do not have access from obtaining such.

Second, formal processes should **include how ePHI access is authorized and how this access will be supervised once granted**. HIPAA-mature organizations rely on peers and leaders to maintain technical and physical security controls around workstations and other devices that access ePHI. CE and BA may identify alternate means to satisfy this HIPAA citation, but we do not recommend informal processes except in the case of a very small workforce (e.g. a single provider practice, etc.), where ePHI access is easily managed.

Third, **apply processes to determine correct ePHI access**. We've seen hospital leadership positions (e.g. CEO, CIO, etc.) with full EHR record access and no functional need to access every patient's record. **Consider pre-employment background checks** to ensure new employees were not previously fired for HIPAA violations and that their credentials are in good standing. When possible, **only grant access to those patient records associated with a position or function and have processes in place to grant emergency access to other records**. Some vendors have not yet built these two controls into their product, so ask if these features are present if you are considering a new software ePHI program.

Lastly, **ensure all ePHI access policies, procedures and processes consider and do not violate any of the other HIPAA Security Rule citations**.

Still Intimidated to Start Your Program?

Develop Policies and Procedures

- Crosswalk every HIPAA citation
- Communicate your intentions (policy)
- Assign key positions and hold them accountable to create the processes (procedure)
- Don't be afraid to ask us for help!

Train Your Workforce

- Develop position-appropriate training across the organization
- Keep training short and focused
- Your policies, procedures & processes are key

Conduct a Security Risk Analysis

- Use a NIST SP800-30 approach
- Crosswalk every Security Rule citation
- Realize the relationship between non-compliance and risk
- Partner with Proteus for your first couple of analyses, then work toward a self-sufficient program
- Manage identified risk and document actions: avoid, transfer, remediate or accept

"If you think compliance is expensive – try non-compliance."
Former US Deputy Attorney General Paul McNulty

Two Companies Learn OCR Accountability Surpasses End of Life

Two recent Office of Civil Rights (OCR) resolution agreements (RA) highlight the impact that an unauthorized disclosure event can have on a CE or BA. In both cases, the businesses were still held accountable, even though one went out of business and the other declared bankruptcy.

- In December of 2017, 21st Century Oncology (21CO) agreed to a $2.3M settlement in lieu of a civil monetary penalty and had to adopt a two-year corrective action plan to settle potential violations of the HIPAA Security and Privacy Rules. 21CO filed for Chapter 11 bankruptcy in May of 2017 but still had to obtain the bankruptcy court's permission to enter into their settlement agreement.
- This February, Illinois based Filefax, Incorporated was involuntarily dissolved. The court appointed receiver has agreed to pay $100K from the estate to settle Filefax's potential HIPAA Privacy Rule citations.

It is our experience that OCR considers the financial health of an organization as part of the RA process. These two cases clearly demonstrate that it's not a reasonable business strategy to "close the doors" rather than develop a program to protect patient information. While not directly mentioned in either settlement, do not forget that since the implementation of the HITECH Act into HIPAA, individual people can be held accountable for their actions.

Articles by Alan Davis
Proteus Consulting
Hayden, ID 83835
(208) 215.5607