Keys to Preventing a Breach

February 20, 2019

For the first time, a former Proteus Consulting client has suffered a major unauthorized disclosure event (i.e. breach) and is now listed on the Office of Civil Rights' (OCR) Wall of Shame. It's difficult for us not to take this news hard, *even though we haven't worked with this Covered Entity (CE) since the summer of 2016.*

Unfortunately, we have no idea of the extent to which they advanced their program or followed our recommendations over the past 2.5+ years – and if this CE enters into an OCR settlement, it may be another two or three years before anyone knows.

After consideration, we feel it is most productive to share some talking points that may limit the damage caused if (when) your company experiences a reportable breach.

The Importance of Your Incident Management Plan

A CE's ability to identify or manage a breach begins with a well thought out incident management plan. The incident management process begins with a workforce trained to recognize and report security incidents. For those not aware, a security incident is:

> *The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.*

An incident management plan includes the workforce members required to investigate, document and report HIPAA-based security incidents, and includes additional resources based on the incident's specific findings. For example, the information services team may need to isolate a workstation, server or email account without delay. The communications staff may need to begin a project to manage a breach's news to affected patients or to the media. The HIPAA Privacy Officer should be integral to determining whether an incident is also a violation of policy and whether a breach has occurred. HIPAA-experienced legal assistance should be pre-defined and ready to help craft OCR responses. The HIPAA Security Officer should be coordinating and owning all aspects of the work involved. Lastly, the incident management plan also needs to be tested against a handful of trending scenarios including both a ransomware or phishing attack.

The Takeaway?

Security incidents "handled by administration" or by an inconsistent or ad-hoc process will either fail, or significantly and negatively affect a CE incident response. If your security incident policy, procedures, and plan doesn't pass a risk analysis – fix this immediately.

The Importance of Effective Workforce Training

Effective workforce training doesn't mean every employee annually checking off their hour-long HIPAA Privacy module developed 10 years ago, supplemented by a couple of periodic staff meeting reminders. The HIPAA Security Rule specifies that a Covered Entity:

Implement a security awareness and training program for all members of its workforce (including management).

Worth repeating is that *to begin with*, the entire workforce needs to be trained to recognize and report security incidents, violations of administrative policy, and potential (e)PHI breaches. The entire workforce should also receive regular short-interval training that teaches protection from malicious software and credential monitoring and management (e.g. logins, passwords, etc.), based on policy, procedure and current information services accepted practices.

Additionally, we wrote about phishing extensively on our website's blog page. Every CE should run a quarterly phishing campaign until the number of workforce members "lured" is reduced. Once responses have plateaued, quarterly testing can be relaxed to an annual or semi-annual periodicity.

The Takeaway?

All CE should already be developing, assigning, and documenting training to learn the HIPAA Security Rule's citations to those workforce members entrusted with each citations' related policies, procedures, and processes. Quarterly phishing training should be budgeted and executed.

The Importance of the Risk Register

The output of the HIPAA mandatory risk analysis should be a risk register that explains each risk that is spawned from a vulnerability (the lack of a sufficient security control). Once identified, risk must be managed and action taken — not just made into a good intention.

Recognizing that there may be more risks identified than there is time to handle each, tackle the highest-level risks and consider finding a part-time employee or contractor to reduce the CE risk profile below a risk tolerance threshold. The failure to properly manage and update a risk register may result in OCR finding "Willful Neglect" during an audit or investigation.

There are four OCR accountability levels used to base a corrective action plan or civil monetary penalty, of which the most expensive is "Willful Neglect." Willful neglect penalties not corrected within 30 days beginning on the first date the CE liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred are $50,000 *per violation*, capped at $1,500,000 for identical violations *per year*.

Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

The Takeaway?

It is human nature to believe that breaches and OCR settlements will only happen to someone else. But the fact is that *a small-sized CE's breach drove the creation of this whitepaper*.

The Office of Civil Rights' Last Announcement Demonstrates Their Resolve

The February 7th, 2019 HHS.Gov web post is titled "OCR Concludes 2018 with All-Time Record Year for HIPAA Enforcement." The webpage continues with "…In 2018, OCR settled 10 cases and secured one judgment, together totaling $28.7 million. This total surpassed the previous record of $23.5 million from 2016 by 22 percent…"

The Takeaway?

It's an unfortunate fact that until the healthcare industry starts treating ePHI the same way a bank treats financial information, *criminals are going to continue to breach multiple CE every single week*.

While the number of OCR settlements are under a dozen a year so far, the mean amount paid to OCR in 2018 has increased to more than $2,607,582 and the median 2018 HIPAA penalty was $500,000.

The amount it costs to maintain a visible, demonstrable evidence-based program is pennies on these dollar amounts and an OCR settlement is just a portion of what a CE pays following a significant breach.

You Have a Relationship With a HIPAA-dedicated Consultant

We realize that regardless of how compliant or secure a HIPAA Security program is implemented, an ePHI breach can happen to the most vigilant CE. *How financially liable the OCR finds a CE will directly depend on the CE being able to demonstrate how reasonable and appropriate selected safeguards are implemented and how much OCR concludes the CE's program is compliant*.

PROTEUS is a passionate HIPAA Security based consulting company and as many of our partner-clients know, we always make time for phone calls or email to clarify any forgotten or new detail. Don't hesitate to reach out if you have a question or need additional assistance.

The Conclusion

HIPAA may someday be expanded or included in future GDPR-like legislation. But for now, the HIPAA Rules are the implementation of federal law. CE need to work their compliance and

security program(s) or hire someone to perform the level of effort involved. Working to prevent a breach is much less costly than experiencing a breach without a compliant and secure HIPAA Security program.