CYBER STORM

HOW TO PROTECT YOUR BUSINESS FROM A DATA BREACH AND THE RESULTING CYBER STORM OF FINES, LAWSUITS & CUSTOMER LOSS

PAUL TRACEY

WHY IS HIPAA COMPLIANCE IMPORTANT?

A SPECIAL EXCERPT FROM THE
AMAZON.COM BESTSELLING BOOK

CYBER STORM

CHAPTER 10

WHY IS HIPAA COMPLIANCE IMPORTANT?

BY PAUL TRACEY
Founder, Owner, and CEO – Innovative Technologies

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which was designed to protect the privacy of patient records, is actually an excellent framework for any organization's security plan. It not only addresses technical measures needed to control the physical environment but also emphasizes the administrative processes necessary to secure data.

And the HIPAA Security Rule, first enforced in 2005, is truly the gold standard for security and should be applied across all industries. The Centers for Disease Control and Prevention (CDC) issued it to provide the following guidelines for electronically protected health information (e-PHI):

- Ensure the confidentiality, integrity, and availability of all e-PHI.
- Detect and safeguard against anticipated threats to the security of information.
- Protect against anticipated, impermissible uses or disclosures.
- Certify compliance by the workforce.

Back in 2003, HIPAA was enforced only in the medical field, but financial industries were also held to HIPAA regulations due to their access to protected health information during the accounting processes. In fact, all business associates of a HIPAA-covered entity are subject to compliance. This includes vendors such as a cleaning service that works in facilities where records are stored.[1]

It is refreshing that both California and New York have passed laws for all businesses that mirror many of the core principles in HIPAA. And more states and industries are certain to follow this trend. However, it is crucial for your organization to implement tight safety protocols long before you are legally required to do so. You can't afford to wait the three to five years it takes from proposal to enforcement. Always follow stricter safety policies than the law dictates.[2,3]

Remember, vehicles in the United States weren't even required to include seat belts until 1968. And it took more than 15 years for New York to lead the path and pass the first usage mandate, which applied only to front-seat riders. Consider how many lives were lost while legislators were kicking around the concept of mandating seat belts.[4]

CONSEQUENCES OF NONCOMPLIANCE

Providers held to HIPAA regulations often don't realize that the fines for violations may be less severe if they have taken proper measures to comply, so it pays to make the effort. If a provider has properly trained an employee and received the policy attestation for the issue in question, the fine and/or associated legal actions

[1] Centers for Disease Control and Prevention (2005), Health Insurance Portability and Accountability Act of 1996 (HIPAA), https://www.cdc.gov/phlp/publications/topic/hipaa.html

[2] State of California Department of Justice (2018), California Consumer Privacy Act (CCPA), https://www.oag.ca.gov/privacy/ccpa

[3] New York State Senate (2019, May 7), Senate Bill S5575B, https://www.nysenate.gov/legislation/bills/2019/s5575

[4] Sheldon, D. (2021, June 9), "A Seat Belt History Timeline," *Your AAA*, https://magazine.northeast.aaa.com/daily/life/cars-trucks/a-seat-belt-history-timeline/

can be greatly mitigated. However, if the violation is deemed negligent because training and policy were not in place, the fines can be ten times higher.

Each HIPAA violation can cost from $100 to $50,000, with maximum annual penalties of $1.5 million. The Department of Health and Human Services' Office for Civil Rights (OCR) has created a four-tier structure to determine liability, with level four being the most severe. Factors considered when assigning a tier also include an organization's willingness to cooperate to improve security, the number of people affected, types of data that were breached, and compliance history.[5]

Here are two examples of health care providers that were seriously burned by violations:

In 2019, Touchstone Medical Imaging paid a $3 million fine after OCR and the Federal Bureau of Investigations (FBI) discovered that 300,000 patients' e-PHI was visible online as search engines were able to index the data. The breach could have been prevented if the company put tighter security in place to protect just one server.[6]

In 2021, Excellus Health Plan settled at $5.1 million after hackers successfully used malware to expose e-PHI of 9.3 million people in Upstate New York. It stings a bit to know they are in our region, and we could have helped to prevent this – and for a lot less money![7]

In addition to the expense, noncompliance hurts your reputation. Details of all violations permanently appear on the publicly

[5] Alder, Steve (2021, January 15), "What are the Penalties for HIPAA Violations?"- *HIPAA Journal*, https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

[6] Cohen, Jessica Kim (2019, May 6), "Medical Imaging Company to Pay $3 Million HIPAA Fine," *Modern Healthcare*, https://www.modernhealthcare.com/technology/medical-imaging-company-pay-3-million-hipaa-fine

[7] US Department of Health & Human Services (2021, January 5), "Health Insurer Pays $5.1 Million to Settle Data Breach Affecting Over 9.3 Million People," press release, https://www.hhs.gov/about/news/2021/01/15/health-insurer-pays-5-1-million-settle-data-breach.html

available Wall of Shame. And a breach doesn't have to qualify as a HIPAA violation to be catastrophic. It may still result in data loss, costly downtime, and a ransom to pay.[8]

REASONS MANY COMPANIES DO NOT HAVE ADEQUATE CYBERSECURITY IN PLACE

Most companies that we initially speak to don't know what data they hold or where it's located in their systems. You can't possibly secure assets if you don't know your inventory and where it's stored.

Let's say someone bursts into a warehouse and steals $100K in motorcycle parts. The thief gets away with it because the boxes weren't properly labeled and never got logged into the system. Since the company didn't keep track of the merchandise, they never installed high-security locks and cameras to protect it.

Companies have misconceptions about which data is being protected. A client may tell us they store all their medical data in an electronic health records (EHR) program, then invite us to perform an audit. We scan their systems and assign a dollar value to the type and scope of e-PHI, then calculate a total liability. We find $2 million worth of medical information saved in downloads folders and other unencrypted locations – all outside the EHR.

And few companies have the time to conduct proper HIPAA assessments. Consider the small medical practices without any IT staff at all and only one office manager. The only HIPAA compliance this person has the bandwidth to do is to fill out the annual questionnaire.

Even in organizations large enough to have an internal IT department, employees are overwhelmed. In addition to their regular responsibilities, they have to install patches to fix

[8] Maheu, Marlene M. (2021, Jun 10), "HIPAA Wall of Shame: See Who Has Violated HIPAA," Telehealth.org, https://telehealth.org/hipaa-wall-of-shame/

previously identified security holes. And they face the looming possibility of a new “Zero Day” attack, which can tie up the entire department for days or weeks.

There’s also a lack of interest. Let’s face it – the HIPAA packet is not making any summer beach read list. At 80 pages, how many employees take the time to review it, ask questions and ensure comprehension before signing their name to attest they’ve done those things? The executive director, legal staff, and a few board members might read the document, but do they ensure that everyone in the company knows their role in compliance? Not likely.

Cybersecurity inequity is highly problematic. Sadly, some organizations cannot afford essential IT services. On average, medical institutions allocate 7% to 10% of revenue to their tech budget. However, most educational institutions only spend 1% to 3% of revenue on technology resources. School budgets simply lack the funding to properly secure their networks. In 2020, grants were available for hardware expenses related to working and teaching from home, but the scope was limited and did not provide much relief. Compare this to the average ‘tech spending’ across all industries, which is 5%.

THE GREAT TECH CRUNCH OF 2020

If security measures were loosely followed before the pandemic, consider the disaster that began in March of 2020. When states, counties, cities – and even entire countries – issued stay-at-home orders to prevent the spread of Covid-19, we had insufficient time to prepare. The majority of workers with jobs that could be done remotely only had in-office setups, so there was a mad rush to get computers home and deployed. At first, due to high demand, it was difficult to even procure the equipment. There weren’t enough chips, and PCs were on backorder. Supply chains could not keep up.

When chips were available, many of the urgently deployed work-from-home (WFH) computers were not set up with proper security, firewalls, or other protocols. And as often happens when pressed for time, many people skipped steps and made mistakes. No one expected perfection, though, because we had life and death on our minds. This is understandable, but as time goes on, the consequences will be catastrophic. Many companies are about to suffer big-time as a result of being in a rush to get s--t done. Sadly, the IT world's neglect is leading to its own self-inflicted global crisis.

No one was prepared for WFH en masse. As an increasing number of companies catch up with audits, we will inevitably learn that a ton of organizations did not give their employees secure home setups. I predict a giant spike in the number of dark web credentials that will be found over the next year. Note that there's a delay in the underworld too, so don't think you're in the clear just yet. If they got you in 2020, credentials such as usernames and passwords will eventually show up for sale.

Another problem with the instant shift away from the office environment was that companies didn't have WFH policies in place. Employees didn't know expectations for online behavior at the home office. They likely reverted to the relaxed mentality usually reserved for time away from work.

Many people tend to take only casual precautions while in their own space – even when using a work computer or connecting to a virtual machine via a personal device. Seemingly harmless actions may include quickly checking Amazon for the price of hiking shoes or hopping onto Facebook to send a birthday message. If non-work-related websites are not restricted, users could be vulnerable and end up visiting malicious sites.

Since a home network is not likely set up with corporate-level security, we are unable to detect or remediate threats that occur outside the office. Home internet connections and public hotspots are typically unencrypted. They are also malicious, making everything you do visible to any hacker.

And cybercriminals loved the widespread surge in video conferencing and saw Zoom and Microsoft Teams with dollar signs in their eyes. They knew the hurriedly installed software was likely not secure. And while Zoom has since locked down security with serious upgrades, they were not ready for the staggering scale of usage. At first, it was riddled with porn pop-ups. (Try to explain that to a third-grader logged into a math lesson.)[9]

IMPLEMENT RULES AND TRAINING AND YOU WILL TRANSFORM THE COMPANY

It's amazing to watch a company's transformation after they adopt a new mindset. For one, the culture can be unrecognizable when you see shifts in employee computer behaviors.

Here's one example of a cultural problem I frequently observe. When I visit a prospect for an intro meeting, I like to chat with people at the company. I note how they refer to the computer they use. If they call it "my computer," this indicates a lack of understanding. It's not *your* computer. It's the agency's computer. It's not *your* data. It's the agency's data. Subconsciously – if you use a possessive regarding a piece of technology, what does your behavior look like?

If you borrow a friend's car, do you drive it with the same care as yours? No, you do not. I guarantee you are more careful. This is because someone else will scrutinize the vehicle to ensure you brought it back in the same condition. If you scratch your own bumper in the parking lot, the beef stays between you and the shopping cart.

[9] Paul, Kari (2021, April 20), "Zoom Releases Security Updates in Response to 'Zoom-Bombings,'" *The Guardian*, https://www.theguardian.com/technology/2020/apr/23/zoom-update-security-encryption-bombing

OUTSOURCE AN IT FIRM

Organizations simply do not have the hundreds of hours per year required to do HIPAA training and implementation correctly. We recognized this and realized we could provide a solution – a package that freed up clients' time. It allows the company to only allocate 15 to 20 hours per year to HIPAA compliance. We do the rest.

We run scans, install security mechanisms such as firewalls and antivirus software, create policy attestations and file reports. We hold training sessions. We even partner with a compliance group that offers audit response should they need it.

We also gamify our security practice. We send employees a three- to five-minute video with a cybersecurity TipTech and run analytics to find out how many people watched it. And we use a tool that simulates phishing attacks to catch dangerous employee behavior. If they click the link or download the file, they get locked out of their e-mail and are instantly enrolled in training. We let internal management know which employees are following safety protocol and putting in the time to learn from the videos, and ask them to recognize those people in front of others.

CONCLUSION

In general, the workforce is significantly undereducated about technology. More training is essential to prevent cybersecurity breaches. Most people do not realize how much time it takes to make sure a company is safe or that most internal IT departments are too busy to do the compliance work right.

Bottom line, you have to hire someone. I'm not here to do a sales pitch, but I'm here to let you know that you could lose everything if you blow off precautionary measures. You absolutely need to keep your data locked down. And there's no time to drag your feet. Please take cybersecurity seriously. And find at least one geek who is willing to read that 'damn' 80-page book and tell you all you need to know.

CYBER STORM

FEATURING

PAUL TRACEY

Paul Tracey is the founder, owner, and CEO of Innovative Technologies. He has seen cybersecurity disasters he wishes he could ‘unsee.’ While at a large healthcare institution, he discovered the department head infected the whole place with malware via his personal laptop. One person made a single mistake, and it cost half a million dollars. Through this experience, he began to notice that while most companies may have some type of security protocol, when compliance interrupts expedience or convenience, managers circumvent the rules. If the organization is wealthy enough, in the event of a breach, they pay the fines, make minimal changes, and carry on.

Not all businesses, though, have the means to survive an attack financially. And the data loss alone is enough to sink them. They are more likely to end up like an engineer he met recently when buying his used office furniture. He was selling it all because he had to shut down his firm. He said, “Man, I wish I’d met you six months ago. We got hacked, and I had to close my business.” The man had lost everything. Every day, sitting in a chair and at a desk, the man and his dismantled team no longer need the visceral and unsettling reminder of the cautionary tale that informs the reason Paul does this work.

You may wonder, how does a company go from thriving to bankrupt in a matter of months? Simply put, most organizations do not make time for security.

The fact that sizable organizations do not take cybersecurity seriously didn’t sit well with Paul. And the imbalance that made it difficult for small to mid-sized entities to thrive was infuriating. He couldn’t bear to stand by and watch them suffer. In turn, building on IT industry experience, studies in information technologies and business at SUNY Adirondack, he founded Innovative Technologies. His company provides technology solutions that minimize security risks for smaller health care providers and other SMBs in Greater Albany, New York.

Nearly a decade later, Innovative Technologies continues to help clients ensure they have security and compliance procedures in place and a well-trained staff. They have earned the reputation as a leading managed security services provider (MSSP) in Upstate New York.

Paul renews his HIPAA Seal of Compliance Verification annually and offers his knowledge as part of the company’s compliance program. He is the author of *Delete The Hackers Playbook*, written to educate the public about ransomware, based on his success in protecting clients from falling victim to paying for data restoration. (https://www.upstatetechsupport.com/cybersecuritybook/)

In his community, Paul served the Glens Falls Greenjackets Semi-pro football team as chief technology officer and board member. Innovative Technologies sponsors the team and also donates annually to St. Jude’s and several local nonprofits.

Profound honesty, transparency, and humility are values that permeate Paul’s work. And the sign on his office wall, “Never Stop Auditing,” applies beyond the literal to his practice of perpetually seeking solutions.

Contact:
Innovative Technologies
Malta, New York (Saratoga County)

- Email: info@upstatetechsupport.com
- Web: https://www.upstatetechsupport.com
- Phone: 518-900-7004

The authors of this book have donated all royalties to St. Jude Children’s Hospital.

For more information please visit **www.stjude.org**

DESIGNED AND PRODUCED BY TECHNOLOGYPRESS™
Printed in the USA

$19.95
ISBN 978-1-7369881-5-2
51995>
9 781736 988152