SECURITY STATE OF THE INDUSTRY

An Interview with Stephen Treglia

JD, HCISPP, HIPAA Compliance Officer,
Investigations Section, Absolute

ABSOLUTE™

OVERVIEW

The health sector is rapidly adopting new technologies, from electronic health record systems to interactive patient portals. But with this widespread adoption comes an endless generation of data – sensitive data that is attracting the attention of sophisticated cyber criminals. Stephen Treglia, a Health Insurance Portability and Accountability Act (HIPAA) compliance officer with Absolute, provides his perspective on how HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act are widening the scope of responsibility past the point of care.

> "You have an obligation to your patients beyond care,"

says Stephen Treglia, Health Insurance Portability and Accountability Act (HIPAA) compliance officer at Absolute, a provider of endpoint security and data risk management solutions. "You need to take the necessary steps to protect valuable information. You need to develop a mindset from top to bottom."

A former computer crime unit prosecutor, Treglia's career has run parallel with the emergence of complex digital systems in regulated industries. His current role was created to help clients navigate and understand the new wave of compliance changes.

WHY ARE CRIMINALS TARGETING HEALTH ORGANIZATIONS?

Unlike financial institutions who were quick to institute secure mobile services, the health industry lags behind in security due diligence. Not only do credit cards and online banking accounts have more frequent activity and monitoring, they offer less information compared to that of a patient health record.

"Not only is access to health records easier for criminals, they are far more valuable," Treglia says. "It fills out the dossier of the impersonator, providing a deeper background on who they say they are," which opens more channels, like Medicaid or Medicare, for fraudulent crimes.

HIPAA RULE CHANGES: A GREATER WEB OF RESPONSIBILITY

"[Information technology] is a very complex area that is not intuitive to lawmakers. And HIPAA was a great foundation, but it lacked enforcement and required proof of harm," notes Treglia. To address the application of advanced technology, the government passed the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009 to encourage adoption and meaningful use of health information technology.

Additionally, in the fall of 2013, Congress instituted additional regulations (called the "Omnibus Final Rule"), making covered entities responsible for the security assessment and compliance of all their business associates.

"The rule states that as soon as you lose control of critical data, a breach is presumed," Treglia explains. Now, notification of a breach is required unless the company can establish a low probability that the data was accessed or transferred by an unauthorized person.

You are guilty until proven innocent, which is why we offer investigative services," Treglia says. "We have over 40 investigators who work with law enforcement agents around the world to help clients recover stolen devices, or at the very least, provide a window of access to control the device remotely."

This opportunity to determine the nature of an incident is critical for businesses, as the penalty per breach is $1.5 million, especially considering many incidents may simply be an authorized person using a device registered in a different coworker's name out of convenience. Or, sometimes security software is not disabled before a device is sold. Neither of these scenarios are HIPAA violations, but without proper evidence, they could still result in a fine.

PREPARE FOR 2016 AUDITS

To complicate matters, the Office for Civil Rights recently announced that "The 2016 Phase 2 HIPAA Audit Program will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules."

On top of that, the HITECH Act also awards power to state attorneys general to obtain damages on behalf of state residents and order other violations of the HIPAA Privacy and Security Rules. As Treglia points out, "This is important to note because they have the authority to suspend business operations within their states."

These audits can be very costly if you aren't up to date on these compliance changes. Treglia notes how the loss of a single laptop cost a company over $100 million in damages and the right to operate in the state of Minnesota. The laptop was left in the trunk of a rental car and stolen. The company had to pay out a $2.5 million HIPAA violation settlement for losing control of the device, which exposed access to the personal data of 23,000 patients.

The Minnesota attorney general then suspended the company's right to operate in the state for up to 6 years. Following the suspension, the company announced a projected annual revenue loss of about $25 million, which snowballed into a $14 million class action shareholder suit settlement as stock prices plummeted.

And, because the company was a business associate of a covered entity, the latter got hit with another HIPAA penalty of $1.55 million for failing to have a proper HIPAA-required business associate contract.

As a HIPAA compliance officer, Mr. Treglia urges all health organizations to review their contracts and follow them to the letter to avoid such situations as this. As he notes, you are responsible for everthing downstream.

STAY IN CONTROL OF YOUR DATA

Remote access to your devices is one way to prevent or limit a data breach. Absolute's Persistence technology is a combination of firmware and software able to track, manage and secure devices remotely.

> "It's a patented solution. We can regain control even after a criminal tries to tamper with the device,"

Treglia says in explaining how the firmware agent automatically reinstalls the security software. "This window of access also allows IT managers to monitor pre-incident clues that can prevent a breach." Such clues include a registry name change on a device and unauthorized software uploads, among others.

"Investing in third party vendors to monitor or track devices is one way to combat potential hackers or satisfy HIPAA rules by establishing the unauthorized data access was due to business travel, not theft.," he recommends.

INTERNATIONAL PROVISIONS IN LIMBO

This past October, the European Union (EU) overturned a 15-year safe harbor practice between the United States and the EU. "Basically, as long as a U.S. company self-certified with the Department of Commerce that they were compliant, the flow of privacy information from EU citizens to the U.S. was allowed to continue without any prohibitions or sanctions," Treglia says.

This changed following Edward Snowden's disclosure about the secret data programs of the National Security Agency (NSA), which allowed the collection of private information directly from companies like Facebook. Max Schrems, an Austrian law student studying abroad in California, questioned Facebook's privacy officer about the EU laws during a school presentation. Unhappy with the answers, he filed suit in Ireland with the European subsidiary of Facebook.

The Ireland High Court acknowledged the problem and supported Schrems' claims, then passed along the greater question to the EU Justice Courts: If there are no real enforcement controls or checks, how could any authority verify that companies that say they are self-certifying with the Department of Commerce are actually certified and following protocol? Disturbed by the discovery that many U.S. companies were not doing what they claimed to be doing, the EU abolished the safe harbor provision.

In February of this year, a new safe harbor provision called the Privacy Shield was written. The Privacy Shield will require the U.S. to monitor and enforce more robustly, working closely with European Data Protection Authorities. And, for the first time, it will require written commitments regarding access to data by public authorities. It has not yet gone into effect, leaving regulators, lawyers and company executives in a legal void.

As a result, the Federal Trade Commission (FTC) and the Department of Commerce have taken on a much more active role in verifying compliance with EU laws. EU Privacy Commissioners will also be held responsible for confirming privacy protections are in place.

The EU has also issued a new, unified General Data Protection Regulation directive for its member countries that goes into effect later this year, carrying a hefty penalty of up to 4% of a company's global profit. Right now, it only applies to businesses who are physically present in the EU countries. After the two-year adoption period, the new provisions will apply to anyone doing business in the European Union, which may not be a concern to hospitals but it certainly will be to medical supply companies and other international organizations.

CONCLUSION

As the industry continues to move forward, dedicate some resources to monitoring industry regulation changes and compliant practices. Whether you hire internally or want to work with a security vendor, the investment will help prevent detrimental damages to your business.

Ransomware and phishing attacks are on the rise. End point security and employee education are key components to preventing data breaches. To limit the damages of a potential breach, every organization should backup their data and have a response plan in place.

In effort to reduce security risks, and enable providers to keep their focus on patients, consider all potential areas of exposure. There is a lot going on right now. Treglia concludes, "Rules are changing quarter to quarter as we figure this out. Proper security and compliant practices will mitigate huge financial losses—whether HIPAA violations or ransom—and ensure health organizations can continue to safely serve patients."

AUTHOR

Stephen Treglia

JD, HCISPP, Legal Counsel
and HIPAA Compliance Officer,
Investigations Section,
Absolute

As legal counsel, Investigations at Absolute, Stephen Treglia provides oversight and guidance on regulatory compliance related to data breaches and other security incidents. Stephen counsels the Absolute Investigations team who conducts data forensics, theft investigations, and device recoveries. Stephen has extensive knowledge of the U.S. regulatory landscape, including SOX, HIPAA, and other industry-specific regulatory bodies.

Prior to Absolute, Stephen concluded a 30-year career as a prosecutor in New York, having created and supervised one of the world's first computer crime units from 1997-2010.

Steve is a nationwide lecturer on legal issues pertaining to technology law, data privacy and security compliance, searching and seizing digital evidence, the admissibility of computer forensic analysis and other related litigation issues.