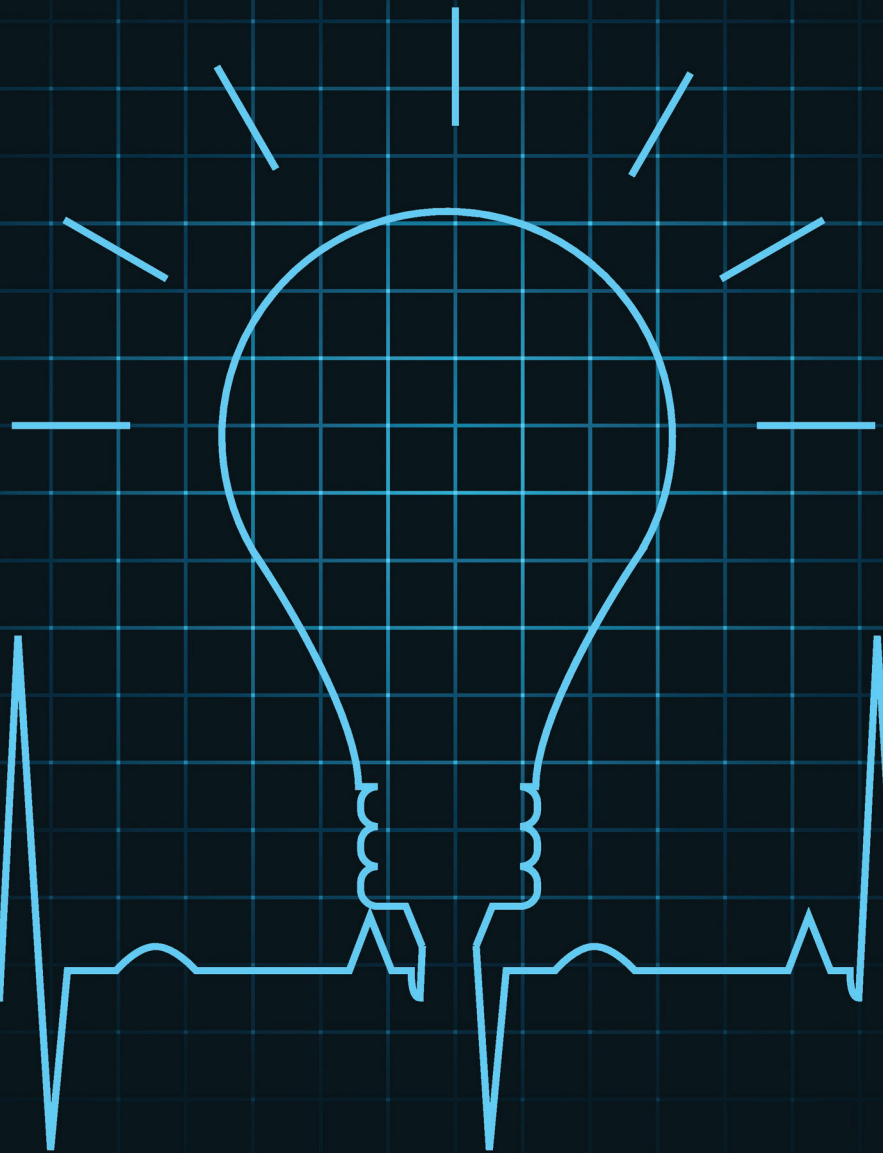# THE CONVERGENCE OF HEALTHCARE INNOVATION AND COMPLIANCE

Scott Whyte of ClearDATA on Achieving the Delicate Balance

With advances in big data, artificial intelligence, machine learning and more, healthcare is primed to innovate. But do HIPAA, GDPR and other regulatory standards inhibit the ability to innovate? **Scott Whyte** of ClearDATA discusses healthcare's complex convergence of innovation and compliance.

"This is a very challenging subject," says Whyte, chief strategy officer at ClearDATA. "But I think there are some ways to break through and get it done." Whyte discusses the high stakes stewardship in play, the challenges of healthcare information security gaps, and stories from leading healthcare organizations working to innovate and improve patient outcomes.

He shares examples of organizations working within compliance frameworks from across healthcare sectors including insights from:

- Global life sciences – An iPad solution for assessing neurological disease progression;

- Behavioral health – A behavioral health pharmacy and largest outpatient telepsychiatry company's solution for rapid scaling, while simultaneously improving security and compliance;

- Payer sector – A large Blue Cross Blue Shield organization engaged in population health and a value-based care initiative.

Compliance Issues

TOM FIELD: With advances in big data, artificial intelligence, machine learning and so much more, healthcare today is in a uniquely exciting time to innovate, but you still have the need to maintain HIPAA and other healthcare compliance standards. In your view, do you find that healthcare is moving away from compliance and more to innovation, or are more cautious organizations opting not to innovate in order to remain compliant?

SCOTT WHYTE: This is a very challenging subject, because I think we would all agree healthcare is so broken that we desperately need innovation. At the same time, we must have compliance. We are stewarding very, very sensitive and personal information.

I do see that organizations are able to take on the issues of innovation and experimentation and agility using novel tools, while at the same time trying to maintain compliance. Now, that is really difficult, and some people get nervous about one side or the other and they shy away and back off. But I think there are some ways to break through and get it done.

Scott Whyte

Whyte, a veteran health IT leader, has more than 25 years of experience serving the nation's largest life science, provider, payer and health solutions organizations. At ClearDATA, he is responsible for driving innovation, growth and strategic relationships. Additionally, he actively advises early stage health technology companies and private equity investors on health technology. Prior to joining ClearDATA, he was an IT vice president at Dignity Health, the fifth largest not-for-profit hospital system in the nation with annual revenue over $12 billion.

from security, privacy and compliance perspectives.

Security Gaps

FIELD: Scott, according to PricewaterhouseCoopers, 74 percent of healthcare providers believe their security activities are effective, but then after an audit, only 22 percent actually meet all the advised security criteria. Do you find that most healthcare organizations that you encounter have gaps in their data security?

WHYTE: Absolutely. We … find that most healthcare organizations have gaps. It's the old adage, "You don't know what you don't know." It helps to have subject matter experts come in and take an objective outsider's view and evaluate your situation.

When I was a healthcare IT executive, I did this. I brought in others—auditors, if you will—who are specialists in the areas of security and compliance to take a look, top to bottom. It's the right thing to do.

Path to Innovation

FIELD: Scott, coming back to innovation, do you find that there's a path forward to be safe, to be creative, to innovate and bring new solutions to healthcare in a HIPAA compliance framework? If so, do you find that it's specific to one healthcare segment, say payers or providers?

WHYTE: It is not only possible, but it is happening. I know of multiple segments in which it is happening. I think it's very possible to address them. I've seen examples in global life sciences, for instance, where an organization is using an iPad solution to assess disease progression in multiple sclerosis. They wanted to roll this out securely in a compliant fashion, not only

A Lot at Stake

FIELD: Scott, we're talking about healthcare here, so clearly lives are in the balance. There's a lot at stake, then, if innovation doesn't succeed, correct?

WHYTE: Oh, absolutely there is a lot at stake—a lot at stake at many levels. You think that if we slow down innovation, there are lives that are lost; there are dollars that we can't save; there are patients that don't have access because we are overly cautious with implementing innovation and new solutions. At the same time, we must be so diligent, because if we experiment recklessly, then we are breaching our patients' trust. We are putting their lives at risk.

Some of our systems monitor patients in an intensive care system, or acute care system or even remote monitoring while they're at home. You can't have those systems be experiments. They need to be rock solid from a time and responsiveness perspective, technically. Very importantly,

they need to be dialed in from a compliance perspective.

We have to know that bad actors who are very actively trying to get into healthcare systems are kept out and that information is encrypted in motion and at rest. We have to know there are multiple layers of security that are in place so that if, by chance, one element gets breached, there are more layers that protect this very sensitive data. We have to think about even the brand exposure for organizations. Some of these organizations have been serving healthcare for well over 100 years, and it's important that they continue that mission.

If they're exposed, if they're breached, they end up on the HHS "wall of shame" as examples of organizations where millions of records have been breached and released, exposed out to the public. There are fines up to millions and millions of dollars, both civil and regulatory, or criminal penalties for these exposures. Yes, there's a need to move quickly for innovation, but yes, there is great care that we must provide

> "It comes back to the point of bringing in subject matter experts, people who've wrestled with these types of problems before, who have the deep security experience."

in the United States with the business associate agreement and complying with HIPAA, but also in the European Union, complying with EU directives. That may seem like a daunting task, but it's absolutely doable.

Again, it comes back to the point of bringing in subject matter experts, people who've wrestled with these types of problems before, who have the deep security experience, the deep compliance experience, and then in this case, the cloud enabling tools and automation in order to perform a global rollout. I've also seen examples in the payer sector of the healthcare market where, for instance, a large Blue Cross Blue Shield organization wanted to boldly engage with … hospital systems that prior to this had been really competing with each other, engage with independent physicians, and help equip them to better manage their populations to measure the quality of care, to exchange data to improve the quality of care, to come up with scorecards and demonstrable results to populations.

That's a challenge, and that type of data exchange can create some complex compliance issues. Again, with the subject matter experts, and some work and the right tools, those things can be addressed. We've seen issues and opportunities with academic medical centers and with software solution companies. There are so many creative organizations that are addressing everything from personalized medicine to accessibility of clinic appointments. There are ways to drive innovation in all sectors of the market while still paying attention to compliance.

Find the Right Approach

FIELD: Scott, it's clear from what you're telling me innovation and compliance don't have to be an either/or. It's both. Now, do you find organizations are taking a do-it-yourself approach, or working in tandem with other SaaS providers?

WHYTE: I see instances of both. Part of the beauty of the cloud is that there are some really powerful tools that are offered. We'll often see … academic medical centers, for example, where they put together some of these tools on their own and did some development and testing experimentation to build an application to help address a certain disease condition. There was some do-it-yourself approach there. When they went to move into production, not surprisingly, their security compliance legal teams wanted everything dialed in from a technical perspective in terms of audit logs and intrusion detection and patching of the operating system. All of those things are a lot of work.

Also, legal agreements. Is there a robust business associate agreement? Is there cyber liability insurance? You need all of those things to make sure that the organization is protected.

Often when they move from that experimentation stage to the stage of actually providing these solutions with real, live patients, for real, live clinicians and caregivers, then they'll want to bring in a partner and help them make sure that the system is designed, built and then maintained in a compliant fashion.

ClearDATA Offers Assistance

FIELD: Scott, we've covered a lot of topics here, but we haven't spoken that much about ClearDATA. Talk to me about what you're doing to help healthcare organizations find this balance between compliance and innovation.

WHYTE: We truly have a passion at ClearDATA for making healthcare better every day. Every person in the organization is focused on that mission, and we specifically focus on our part, which is the security, privacy and compliance of the cloud.

We conduct security risk assessments, bringing in our subject matter experts and helping assess environments and applications at hospitals, physician offices, payers and pharma organizations to provide insights into where they may have gaps and to provide recommendations for remediation.

In addition, importantly, we provide the design, the build and the ongoing management of cloud environments. These are the foundation for many of these innovations that we discussed earlier; they're the foundation for solid privacy, security and compliance.

We have tools like our security and compliance dashboard, which gives insight into the status of the underlying cloud environment and the platforms that serve applications and solutions in healthcare. Those dashboards give specific mapping – for instance, red, yellow, green – on how that environment is meeting specific subsections of the HIPAA code of federal regulations – or in the case of pharmaceutical or medical device solutions – whether those solutions are compliant with FDA or GxP requirements.

These are solutions that we're excited about delivering to hospitals and payers and pharma organizations in the United States, in Canada, in Europe and Asia, and we're thrilled that even some of those examples that I mentioned earlier are actually ClearDATA customers. ∎

Listen to the full interview at: https://www.bankinfosecurity.com/interviews/convergence-healthcare-innovation-compliance-i-3875

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io