healthcare informatics
CUSTOM MEDIA

Searching for Security:

The Importance of Planning and Maintenance for Longterm HIPAA Compliance

Research Supported by:

Connection™
we solve IT™

Contributing Executive

Bill Virtue

Security Engineering Specialist

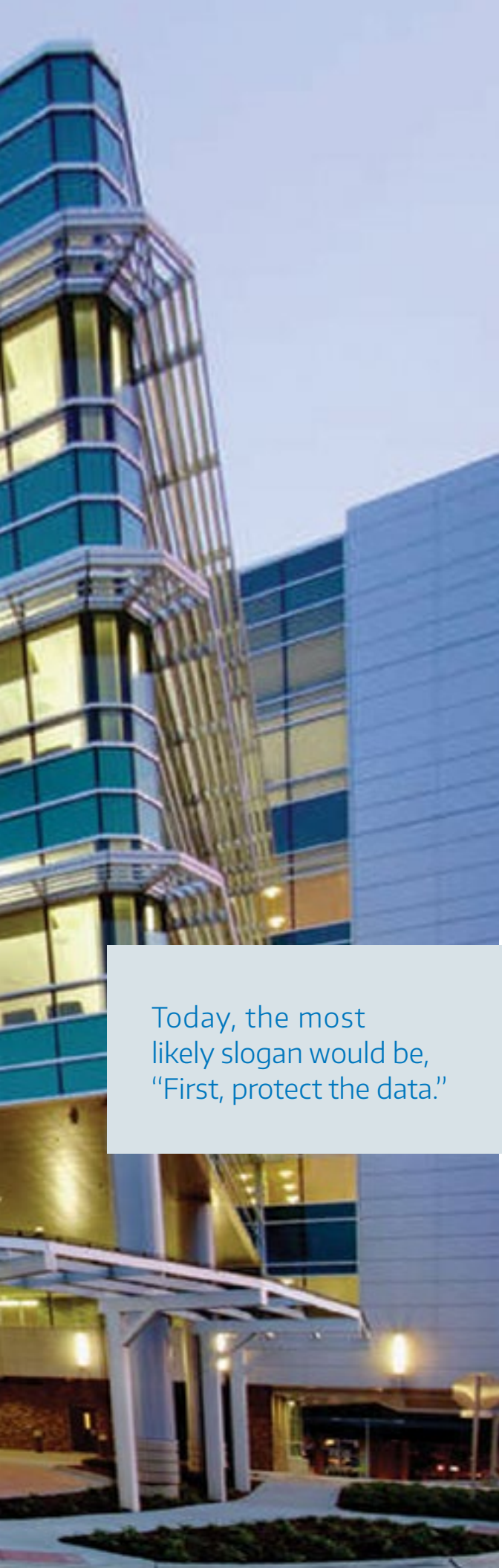
Connection

Executive Summary

Today's healthcare landscape brings many challenges. While more and more technologies are available to help healthcare organizations manage the rules and regulations put forth by the Health Insurance Portability and Accountability Act (HIPAA), no one single security control, no matter how state-of-the-art, can do the job by itself. Success depends on the implementation of a variety of different security controls—as well as strong maintenance and enforcement policies—to protect organizations from both internal and external threats.

There is no question that healthcare organizations that do adhere to strong security programs are more likely to protect private health information (PHI) – and avoid an expensive and time-consuming security breach. And providers who have executed robust security processes around HIPAA analysis and compliance, with ongoing management of those processes for monitoring and risk mitigation, are reaping the benefits.

The purpose of this white paper is to better understand why a thorough and robust security maintenance plan is necessary to best meet HIPAA requirements and regulations. It will discuss the costs of patient data breaches—beyond today's exorbitant HIPAA fines. It will highlight the various security controls and technologies currently available to providers, and explain why each is not enough in its own right to ensure data safekeeping. This report will consider the importance of a good security plan—and why ongoing management and enforcement of said plan is crucial to success. And, finally, it will emphasize what chief information security officers (CISOs) and other information technology (IT) decision makers need to know as they formulate their plans for continuous data protection across the enterprise—and avoid costly data breaches that can put both their patients and their business at risk.



Introduction

It's often said that the doctor's prevailing mantra is, "First, do no harm." But given those good words of Hippocrates, words that have transformed the realm of provider care, what words might hospital chief information security officers (CISOs) repeat most frequently? Today, the most likely slogan would be, "First, protect the data."

And for good reason. With the regulations mandated by the Health Insurance Portability and Accountability Act (HIPAA), the costs of a potential data breach are severe.[i] Over the past two years, hospitals across the country have paid millions of dollars in fines for things like the inappropriate disposal of patient health information (PHI), lost or stolen unencrypted laptops, and improper deactivations of network servers.[ii] But Bill Virtue, a Security Engineering Specialist at Connection, says that cost of a breach go far beyond those expensive and headline grabbing fines.

"You also need to look at the cost of remediation. That's something beyond the fine that has a big price tag to it," he says. "On average, the cost of a breach comes out to about $350 per patient record. But, honestly, the cost keeps going up. Especially if you don't have a good plan in place."

Given the staggering—and rising—costs of a data breach, Virtue says that a provider's best course of action is to implement a strong security plan, one that is designed both to prevent a breach as well as to respond and recover from one, in order to manage costs and ensure there are no interruptions to patient care.[iii]

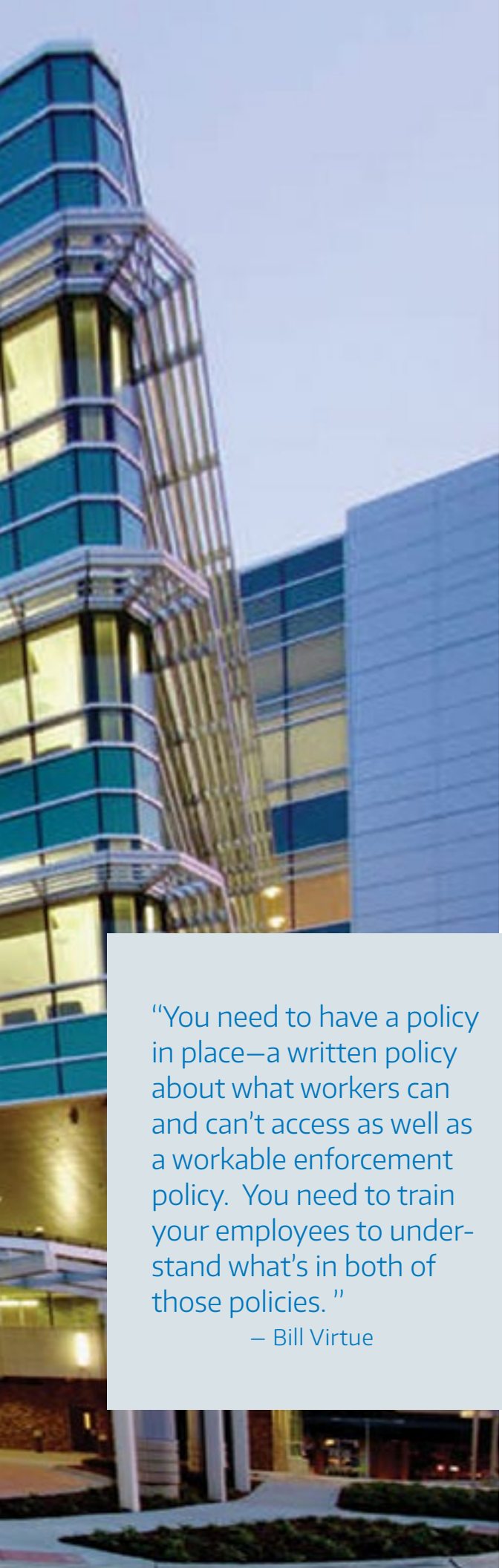
Today, the most likely slogan would be, "First, protect the data."

Several Controls Working Together

Certainly, there are no lack of security controls available to healthcare organizations these days. Hospitals can implement strong password management and access control systems, encrypted hard drives and storage systems, secure network servers, and strict bring-your-own-device (BYOD) policies. But Virtue argues that no single security control is enough to manage PHI security, nor is any one of these controls more important than another. And that is mostly because healthcare tends to be a very fluid environment.

"Healthcare workers have access to PHI data using a variety of systems, mobile and otherwise, on-premise and off-premise. They need to be able to get to the data to do their job but getting access to that data can leave an organization vulnerable," he says. "The challenge is understanding who the people are who are accessing patient data, where they're located, how they get access, and what they actually need access to. No one control is enough because the answer to those questions may change from day to day. A single healthcare worker may be accessing a certain kind of data from a certain place one day and then doing it a different way in a different role on another. You have to account for that."

For example, a healthcare worker may be working out of a surgical floor in the hospital one day, trying to access data from a mobile device to help deal with the hustle and bustle of surgical suite—and then working on a desktop system out of a provider office the next. A specialist physician who is called in to the emergency department for a consult may need to access data from imaging systems managed in the radiology department—and then port that data back to his office or home department for further examination. As healthcare organizations continue to merge and



partner in different ways, those roles continue to evolve. This can make managing and maintaining identity and access difficult.

"It's not as easy as it may seem. The HIPAA mandate has some hard-nose items that your organization must do when it comes to data. But it also has a bunch of items that you an address in different ways or even find workarounds for," he says. "So you need to have a policy in place—a written policy about what workers can and can't access as well as a workable enforcement policy. You need to train your employees to understand what's in both of those policies. But because healthcare workers aren't focused on keeping PHI safe, they are focused on taking care of patients, that training often isn't enough. You really have to work to help healthcare workers treat patient data the way they are supposed to."

But creating such plans are no easy feat. Beyond a flexible environment, healthcare is also seeing record changes in terms of connectivity. Breaches can come both from the inside, with healthcare workers not appropriately protecting PHI, and from the outside, with hackers trying to find entrée to your network. Providers must consider all points of potential access in their security plans including other provider partners, health information exchanges (HIEs), accountable care organization (ACO) networks, vendor partners and medical devices. Only plans that consider all of these elements in a comprehensive and realistic manner can hope to effectively comply with HIPAA requirements.[iv]

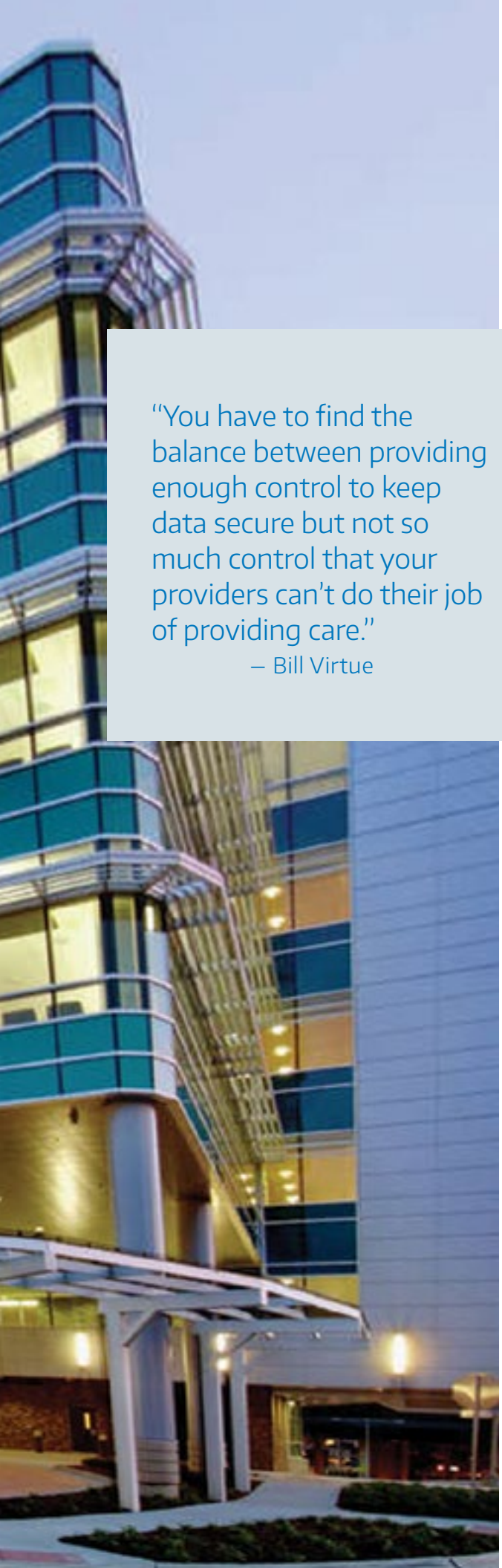
> "You need to have a policy in place—a written policy about what workers can and can't access as well as a workable enforcement policy. You need to train your employees to understand what's in both of those policies."
>
> — Bill Virtue

Putting the Right Plan in Place – and Maintaining It Over Time

As provider organizations attempt to put these complex and dynamic pieces in place while designing their security policies, Virtue says they must understand that policies cannot be simple static documents if they are to be effective. Certainly, hospitals need to get access controls and restrictions right immediately, but they also need to make sure those policies are being actively maintained over time.[v]

"There's a lot here that can be automated. And you can have policies in place to help prevent people from getting into the network and to prevent people from off-boarding protected information out of the network. But, in both cases, you need to really fine-tune your plan. It's never going to be one-size fits all but having strong authentication controls in place are key," he says. "But given that those access controls are key, and are so dynamic, you need to be able to maintain and manage them over time. It can be hard to manage."

That maintenance involves knowing where your data is—but also what users need access to it and how your organization will provide that access in a mobile environment. You need to understand what parts of your access and enforcement policies are automated and how users might get around those controls when and if they get in the way of the provider's job: providing quality care. Simply stated, having a good policy is not good enough. All of those moving pieces need to be maintained over time. And that's where many healthcare organizations fall short.[vi]



> "You have to find the balance between providing enough control to keep data secure but not so much control that your providers can't do their job of providing care."
>
> — Bill Virtue

"You have one provider who maybe moves departments or is working from a partner hospital but you don't change the access controls," Virtue says. "If you don't keep up with that, and maintain that authentication and access even as people move across your organization, you are going to run into trouble. You need to make sure your plan can follow the identities of healthcare workers and they can get to what they need when they need it when they are working in that particular role. You have to find the balance between providing enough control to keep data secure but not so much control that your providers can't do their job of providing care."

More Work Than You Thought It'd Be

Virtue says understanding provider use cases, performing a proper gap analysis, and then creating the right security plan can seem overwhelming.[vii]

"A lot of CISOs are looking at all of the things they need to do, all the things they need to wrap their arms around in order to really be HIPAA compliant, and they are realizing that it is a lot more work than they may have initially thought it would be," he says. "And often they are asking themselves, 'How much is this going to cost me to do myself? How much would it cost me to have someone else do it? Which approach is going to get me where I really need to be?'"

But Virtue says, as many hospitals don't have the right staff to handle tough security initiatives, having the right vendor partners in place can be an advantage to help healthcare providers understand what technologies are available to help them automatically manage and enforce access and security protocols; train staff to not only understand organizational security policies both in theory and practice; and give the IT department the tools they need in order to maintain those policies in the face of a fast-paced and dynamic environment.

"Having the right plan in place helps to avoid any breaches. But if a breach should occur, and it may occur, you also need to make sure that you have the alerts and notifications you need to detect when things go wrong and block suspicious activity," he says. "You need to understand the breach notification laws in your state and what you need to do in terms of remediation. And to make

sure you can do that, you need to take a good look at what pieces you have in place and ask yourself if they are really protecting your organization the way they need to."

First, protect the data. It's the heart of HIPAA compliance.

But to protect patient data, and protect your organization from unwanted and expensive security breaches, you must have the right plan in place. One that – in terms of monitoring, management, and maintenance – will help you ensure that you are continuously meeting HIPAA requirements and mitigating risk.

Supporting Research

[i] https://www.hhs.gov/hipaa/for-professionals/index.html

[ii] http://www.beckershospitalreview.com/healthcare-information-technology/15-of-the-biggest-data-breach-settlements-hipaa-fines.html

[iii] http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

[iv] https://www.pwc.com/us/en/health-industries/top-health-industry-issues/assets/2016-us-hri-top-issues.pdf

[v] http://www.isdecisions.com/healthcare/compliance-research-executive-summary.htm

[vi] https://hitrustalliance.net/content/uploads/2015/09/ImplementingNIST-CybersecurityWhitepaper.pdf

[vii] https://www.gartner.com/doc/2706021?srcId=1-3931087981