WHITE PAPER

8x8, Inc.

Why HIPAA Compliance Should Scare You and What You Should Ask Your Business Phone Service Provider NOW

By Mike McAlpen, 8x8 Executive Director of Privacy, Security and Compliance

Contents

Why You Should Ask Your Business Phone Service Provider about HIPAA Compliance

What is HIPAA, how does it relate to business phone systems, and why should you care?

Federal regulations have changed, and your compliance burden might have increased without your knowledge.

The Health Insurance Portability and Accountability Act (HIPAA) provides federal protections for Personal Health Information (PHI). As of January 2013, HIPAA covers not only the traditional "covered entities" such as medical providers and payers, but any of the entire chain of third parties that create, receive, maintain or transmit PHI, also known as "business associates." In other words, the scope of the regulations are broader and now cover many more people and businesses than before.

The law requires all of these entities to safeguard the confidentiality, integrity and availability of this private information through a variety of means, such as encrypting patient record PHI or insurance information stored or transmitted by computers.

HIPAA compliance used to be something that mostly affected healthcare and directly related businesses. Now, any company that creates, receives, maintains or transmits PHI—which is turning out to be the majority of US companies—must comply. This includes business phone service providers, including VoIP services.

Enforcement is also being stepped up. In January 2013, the latest Omnibus Final Rulings update to HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH) Act expanded their regulatory scope and added more random audits, as well as stiffer penalties for non-compliance.

The US government really does care that your phones comply

This brings us back to the question: As a user of business phone service, why should you care? After all, there has not been a great deal of discussion about HIPAA compliance and business communication systems in mainstream venues.

Many of those who are now at risk from these new HIPAA regulatory requirements may not be aware that they are now considered a business associate under these new expanded HIPAA regulations.

But when it comes to phone systems, a lack of awareness about the need for compliance will not get you off the hook, as this is a *law*. If you are a covered entity or one of the thousands of new business associates, and your business communications system is not compliant with these latest HIPAA requirements, your business may be at risk. If your business is involved in an investigation, there could be significant financial penalties and/or federal litigation for not meeting HIPAA privacy requirements.

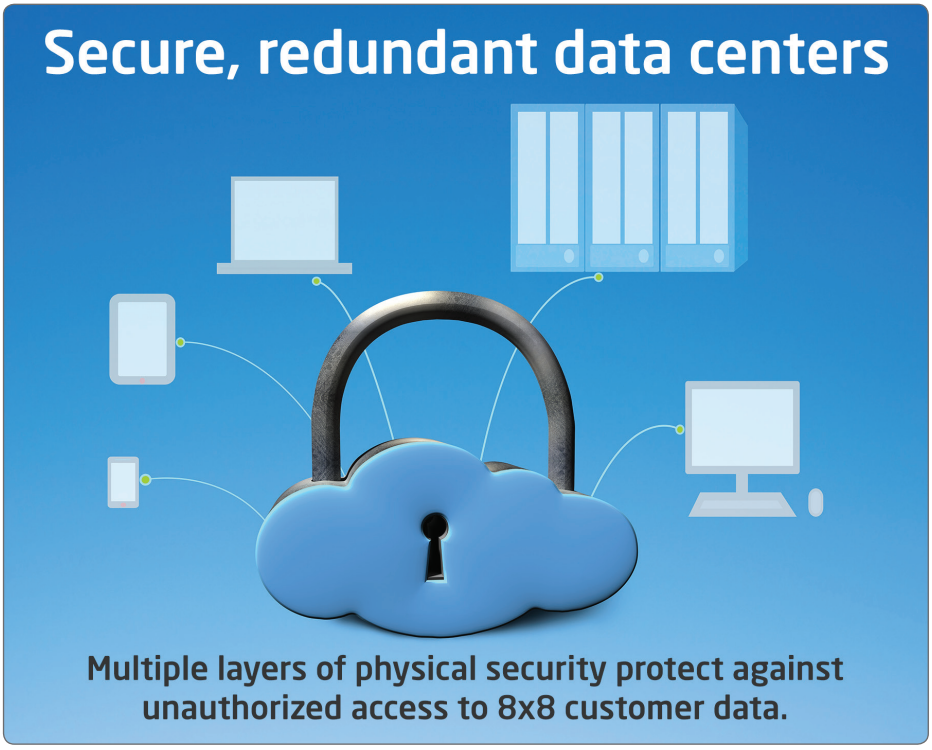
"Unfortunately, many of those who are now violating these regulatory requirements may not even be aware that they fall under these newly expanded HIPAA regulations."

Mike McAlpen
Executive Director of Security and Compliance at 8x8

Even less well known is the fact that these new HIPAA business associates could face regulatory problems due to the compliance violations of companies they do business with. It is now up to covered businesses to negotiate a HIPAA Business Associate Agreement with any of their third parties that create, receive, maintain or transmit PHI on their behalf. To be compliant, all organizations covered under HIPAA must have HIPAA Business Associate agreements in place with all of their partners that handle PHI on their behalf, ensuring that these partners are legally obligated to maintain compliant levels of PHI data confidentiality, integrity and availability.

Your business is responsible for reading the fine print

If you own your telephone switching equipment—like most users of on-premises PBXs—you're responsible for making sure the service is compliant and protects any stored information.



But if you subscribe to telecommunications services, then you must ensure that your service provider is not only a HIPAA-compliant business associate, but that all of your provider's covered third parties are fully HIPAA compliant and have signed Business Associate Agreements with the communications service provider.

And communications services are decidedly not created equal. Some well-known communications solution providers are, in fact, not at all HIPAA compliant, let alone compliant with the latest HIPAA HITECH Omnibus regulations.

This is particularly true with cloud VoIP providers. Many have admitted publicly that when it comes to information covered by HIPAA, their business phone systems "should *not* be used for these purposes." [1] Due to the challenges involved in meeting these requirements, many providers have not even attempted it.

This means that someone at your organization needs to ask the question, "Do our phone, fax, and other communications solutions comply with the latest HIPAA requirements?"

1 RingCentral S-1 filing, SEC, August 26, 2013, p. 28, found at http://www.sec.gov/Archives/edgar/data/1384905/000119312513346260/d310247ds1.htm.

"If you use a cloud-based service, [its provider] should be your business associate."

David Holtzman
U.S. Health and Human Services Department's Office for Civil Rights, Privacy Division

How far will 8x8 go for your security?

Achieving HIPAA compliance takes significant skill, knowledge, experience, resources, equipment and other financial commitments. Many firms just do not have the resources or expertise necessary to attain compliance.

For example, HIPAA mandates protection of data. So, to ensure the security of stored data such as voicemails, faxes, and call recordings, the 8x8 service is housed in multiple redundant top tier state-of-the-art, SSAE 16 certified data centers. Each is staffed 24/7 and equipped with high-grade security features, equipment and procedures. Multiple layers of physical security protect against unauthorized access. These layers include mantraps, biometric hand geometry readers, visual confirmation, and 24-hour video surveillance. 8x8 has gained some of the highest possible levels of third-party compliance validations.

This investment in our customers' protection is part of the reason why 8x8 services can be configured to be HIPAA compliant, with administrative controls and restrictions to protect stored faxes, recordings and voicemails. We also offer our customers optional FIPS 140-2 (Level 2) compliant data-in-motion and data-at-rest encryption.

Why choose a compliant cloud-based VoIP solution?

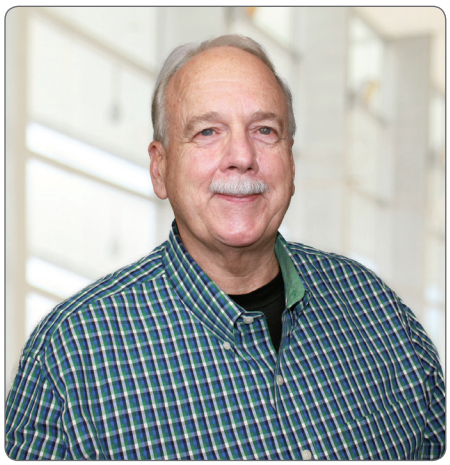
You get two major benefits from choosing a cloud-based VoIP solution from a HIPAA HITECH Omnibus-compliant provider with HIPAA-compliant downstream business associates.

First, a "hosted" or "cloud-based" system is provided over the Internet by a service provider that maintains the solution, so you don't have the overhead of upgrading, managing or maintaining the system. And second, you shift significant aspects of the compliance and security burdens to the provider.

Get it in writing

With steep fines—up to $1.5 million for each egregious violation—many businesspeople are left wondering how to make sure their communications provider is HIPAA/HITECH compliant.

Whether auditing your existing system or evaluating a new service, you should ask the question: Can your communications provider—of business phone service, fax service, call center, web conferencing, etc.—offer a HIPAA Business Associate Agreement (BAA) that is compliant with the latest expanded HIPAA HITECH Omnibus regulations?



About the Author

Mike McAlpen, CISM, is the Executive Director of Privacy, Security and Compliance at 8x8. Prior to that, he was a Senior Director of Global Information Security at Visa. He also works with the FBI and Department of Homeland Security and the U.S. Secret Service's Cyber Crime Task Force. In addition, he is an active member of the American Bar Association - SciTech Law - InfoSec. and Digital Evidence Committees, as well as the eDiscover and Data Governance Committees. A frequent speaker at RSA and other Security Conferences, he serves as a senior member of the board of directors of the International Systems Security Association (ISSA), Silicon Valley, and is a certified member of the ISACA Information Systems Audit and Control Association and a member of the International Communications Fraud Control Association (CFCA). Finally, Mike is a senior member of Secureworld Silicon Valley CISO Advisory Board and an original member of the Cloud Security Alliance (CSA).

BAAs: An important compliance feature

Offering an updated business associate agreement means that a phone service provider is willing to stand behind its compliance and say in writing that it has the proper privacy and security controls in place. Don't settle for anything less, experts say.

"If you use a cloud-based service, it should be your business associate," says David Holtzman of the US Health and Human Services Department's Office for Civil Rights, Privacy Division. "If your business is going to use a vendor that stores PHI on your behalf, you must have a Business Associate Agreement in place. *If they refuse to sign, don't use the service.*"

The rigor with which 8x8 has developed the several types of BAAs it offers is an important service feature. These agreements, based on nationally recognized HIPAA legal expertise, cover all aspects of the downstream compliance issues involved with third-party associates.

The ability of 8x8 to stand behind these agreements—combined with extensive audit trail capabilities within the system—means that 8x8 customers get written documentation that their business communications won't jeopardize their own HIPAA compliance efforts.

Failure to comply is not an option

Choosing a provider that cannot assure that its solution and back-end systems are HIPAA/HITECH compliant—and that can't provide you with the correct version of a fully HIPAA compliant BAA—can put your business at significant risk of heavy fines from regulators.

8x8 cloud-based service doesn't just eliminate the headaches of managing a premises-based phone system. It also addresses HIPAA HITECH Omnibus communications services compliance worries.

Peace of mind

These features offer the further benefit of ensuring the general security of your business communications, while offering you the peace of mind that the compliance experts at 8x8 will keep their solutions updated with all the latest security capabilities and requirements.

8x8 offers the confidence of knowing that your communications are compliant. It also gives you a great answer to the question, "Are our communications HIPAA-compliant?"

For more information, call 1-866-879-8647 or visit www.8x8.com.

8x8, Inc.

NASDAQ: EGHT
www.8x8.com