THE FOGHORN WAY

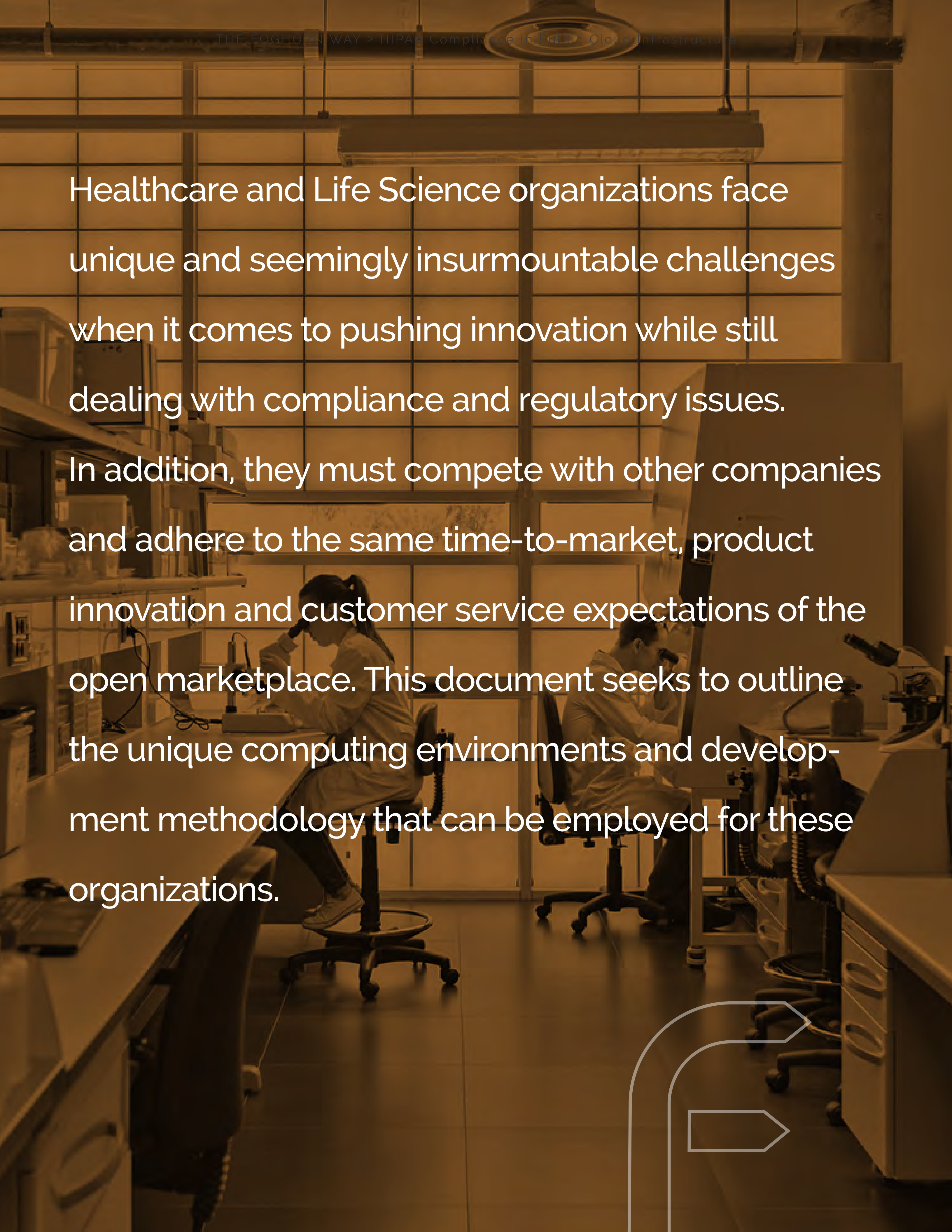
A Resource Guide For Navigating The Cloud

OVERCOMING THE IMPOSSIBLE:

How to be HIPAA compliant in a public cloud infrastructure while still maintaining agility.

SEPTEMBER 2017

TABLE OF CONTENTS



Healthcare and Life Science organizations face unique and seemingly insurmountable challenges when it comes to pushing innovation while still dealing with compliance and regulatory issues. In addition, they must compete with other companies and adhere to the same time-to-market, product innovation and customer service expectations of the open marketplace. This document seeks to outline the unique computing environments and development methodology that can be employed for these organizations.

IMPROVE THE MODEL BY SPLITTING INTO TWO MODELS

Move swiftly or move within compliance and regulatory guardrails? Actually, organizations can do both. Even with limited technical resources, organizations can focus on compliance and still focus on being agile. By separating out use cases between the compliance phase and the "sandbox" phase, it enables a more streamlined approach. Through tokenization or cleansing of the data, organizations are enabling speed for researchers, scientists, doctors, and development teams to get the PHI component temporarily out of the process. For instance, a drug company benefits from splitting out a bevy of simulations and analysis prior to the qualification phase. Similarly, healthcare researchers might test that their algorithms for sequencing are working without affecting potentially protected health information.

Separating out all compliance pieces, and removing those from those use cases, gives researchers, scientists and doctors the freedom to move very quickly without fear of being out of compliance, breaking regulations, or having a violation in HIPAA laws.

Once they have the freedom and speed to operate in a non-validated scenario, it's necessary to look at a completely separate operating model for the next phase: working with PHI in a compliant environment, or requiring a qualified environment. In this scenario, workloads run in a strictly controlled environment where access is limited to those intimately familiar with certification and compliance requirements for the specific workload. Sandbox environments remain agile, with no risk of accidental compliance breach, and qualified environments remain tightly controlled.

HOW CLOUD COMPUTING HELPS BRIDGE THE AGILITY / COMPLIANCE GAP

Infrastructure as code is more than just a concept that helps Healthcare and Life Science organizations use cloud computing to realize their full potential. It's a full-fledged development approach that deftly balances the needs for both agility and compliance. When infrastructure as code is automated via deployment pipelines, the audit trail for compliance is already present. In that same vein, cloud computing enables permission-based controls through the process thus enabling appropriate and role-based access to different infrastructure components.

The CI/CD pipeline is a good example to explore how the infrastructure as code helps balance agility with compliance. The Compliance team can add automatic checks ranging from simple (encryption handling) to complex (scanning of containers or artifacts). In addition, It could also enable certain alerting and logging. The pipeline can have an endless number of checks against delivered items or applications because the access levels have been defined and enforced.

THE AGILE TEAMS STAY AGILE. THE COMPLIANCE TEAMS STAY COMPLIANT.

By codifying all of the elements, you have a commit history of your entire infrastructure stack. Each change has been through peer review by either a pull request or some similar model. Agility teams are coding new features, and then doing peer reviews. Compliance teams are looking at the code from a risk standpoint, change management, and change control. The two teams meet up in the repository to see what infrastructure code has been modified. In this environment, there are scans that can be run that check for certain vulnerabilities and certain compliance requirements. With minimal extra effort, it enables the application team to maintain agility, and allows the doctors and the scientists to accelerate research, simulations, and tests. And once it hits the compliance environment, those folks can focus on the pieces that they are very good at, that they are ultimately responsible, therefore ensuring compliance. The two can operate independent of each other and even in parallel.

CODIFIED AND VERSIONED INFRASTRUCTURE ENABLES BOTH INFRASTRUCTURE AND AGILITY.

SHOULD WE GET HIPAA CERTIFIED? (IT'S A TRICK QUESTION)

Contrary to belief, there's no industry certification for HIPAA. HIPAA is a law. It's a set of guidelines and it's the responsibility of the company who is managing that protected health information to ensure that they're compliant with those guidelines. The solution that many organizations turn to is HITRUST certification. While not specific to HIPAA, HiTRUST is considered a super set to HIPAA guidelines.

WHAT'S HITRUST?

Founded in 2007, the HITRUST Alliance, a not for profit, was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST develops, maintains and provides broad access to its common risk and compliance management and de-identification frameworks, and related assessment and assurance methodologies, as well as programs supporting cyber sharing, analysis and resilience. (https://hitrustalliance.net)

Healthcare organizations are left to wonder: Is HIPAA enough, or is HITRUST certification a requirement for companies moving their HIPAA regulated workloads into public cloud infrastructure?

There are several valid reasons for going through the expense and effort to become HITRUST certified. Many vendors who sell to large healthcare organizations will be required to obtain and maintain HITRUST certification as a prerequisite for doing business. These companies have no choice but to get certified. Even if HITRUST is not a requirement, the certification can be very useful for selling services to companies in the Healthcare vertical. It can be a differentiator, and eases HIPAA compliance concerns.

Larger organizations see HITRUST certification as a tool to assure HIPAA compliance. Maintaining the certification assures that appropriate systems and processes are in place, and are in use.

Two requirements go into obtaining HITRUST certification: First, organizations must have the controls and processes in place. HITRUST scales the requirements with the size and complexity of the organization or solution getting certified which means smaller organizations do not have to invest in financially crippling automated systems but rather can meet requirements by using simple manual processes and logging. The second requirement is documentation of processes and controls. Because HITRUST auditors are required to gather evidence to prove that those systems are in place, organizations must be prepared to turn over actual work documents (i.e., screenshots) and examples to show that their processes and controls are implemented.

The concept of segmenting access and control touched upon earlier applies to the certification realm as well. Because organizations segregate the responsibilities it helps prevent someone who's not trained in understanding the ramifications of their actions, say by changing a security rule, or a changing a network configuration rule, to inadvertently altering its compliance status.

MAKING SURE YOUR BAA IS AOK WITH HIPAA.

As if navigating the intricacies of healthcare data management wasn't difficult enough, it's critical that companies also protect themselves when working with subcontractors or vendors. Companies that handle protected health information and entrust others to handle this information must sign a Business Associate Agreement (BAA) in which those vendors are agreeing, effectively, to treat that PHI as the HIPAA guidelines recommend. If they don't, companies can be out of HIPAA compliance and held liable for that.

How do Healthcare organizations ensure the BAA with the cloud vendor is meeting HIPAA obligations?

Most BAAs agree to protect data or to follow specific rules so that organizations can be HIPAA compliant, only on the condition that the services are used in a predetermined, inflexible manner. This is a key difference of the BAA relationship in the cloud computing world — there are misconceptions about what the BAA actually covers. What this means is it puts the burden back on the consumer of those cloud services to ensure that the BAA is covering the use of these services . And if it's not in place, organizations are no longer protected.

As a result of this inflexibility by the BAA, organizations need ways to protect or implement guardrails and real-time monitoring to further ensure compliance and adherence to the BAA. For some of the cloud vendors like Amazon, a simple way to do that is to actually use account segregation and segregate workloads, PHI versus non-PHI, in different accounts. Organizations would simply limit access controls of the API calls that could be made to those that are under the BAA. However, because the BAA calls out use of certain services that go beyond the simple API command that might be executed, turning off access to services that aren't covered in the BAA is not enough. It is still up to the cloud consumer to assure, in the shared security model of the cloud, that compliant services are leveraged in a compliant architecture. Ensuring, for example, that PHI is encrypted at rest and in transit, that application vulnerability assessments are regularly completed, etc.

In conclusion, by leveraging the key components of cloud computing — namely CI/CD pipelines, infrastructure as code, configuration management as code — you can maintain agility and compliance. This approach further helps Healthcare and Life Science organizations with automation around compliance checks in order to give some real-time compliance and comfort that a qualified environment hasn't changed. Finally, development and qualified environments are separated so that PHI, and other restricted data allows comfort and moving quickly without fear and allowing those workloads when ready to be run in a qualified environment or a HIPAA compliant environment.

The actual knowledge workers, scientists and researchers can work at a very rapid pace without fear of compliance problems.

Data Points:

#1 Factor in choosing a Cloud Services Provider?
Adherence to Regulatory Requirements (HIPAA, HiTECH)

Top Ways to Measure Value of Cloud Services Adoption
> Augmentation of technological capabilities
> Speed to market with new clinical initiatives
> Better regulatory compliance

Source: © 2016 HIMSS Analytics Cloud Survey

Review Your HIPAA Requirements with a FOGHORN Cloud Expert

SCHEDULE A CALL

Foghorn Consulting was founded in 2008 with a mission to ensure that cloud computing initiatives deliver maximum value for its customers. Based in the Silicon Valley, Foghorn provides domain expertise in strategy, planning, execution and managed cloud services to high-growth and enterprise companies seeking a cloud partner. Our team of DevOps engineers, SRE's and certified cloud architects bring over 20 years of domain expertise to ensure your cloud initiatives are a success.

FOGHORN

330 Townsend St, Suite 202
San Francisco, CA 94107
foghornconsulting.com
info@foghornconsulting.com
650-963-0980