David Starr: Welcome to the Microsoft Industry Experience's team podcast. I'm your host David Starr, and in this series, you'll hear from leaders across various industries discussing the impact of digital disruption and innovation, sharing how they've used Azure to transform their business. You can find our team online at aka.ms/indxp or on Twitter @IndustryXP.

David Houlding is the principal healthcare program manager on the Microsoft Industry Experience's team. He has extensive experience in healthcare and applicable technologies, most lately the cloud, block chain, and AI. Welcome to the show, David.

David Houlding: Thanks, David. It's great to be here.

David Starr: We're here to talk about reducing healthcare costs with digital transformations in healthcare, specifically around security compliance and backup using Azure. So, what are some of the key challenges that healthcare is facing right now?

David Houlding: Yeah, reducing healthcare costs is really a major one, and you had it. Healthcare is nearly 20% of GDP in the US, so phenomenally high cost, and it's increasingly expensive worldwide, so we have this huge problem of the non-availability of healthcare to many people, so I think one of the things we need to be doing is driving the availability of healthcare as much as possible to really democratize healthcare and to do that by reducing cost, and IT cost is a significant portion of the overall cost of business of healthcare, so whatever we can do to reduce the costs of information technology is something that we should be focusing on.

And, moving to cloud computing is one way of reducing a lot of cost in IT, capital expenditures, all the resources required to maintain, to procure, maintain, refresh, low level infrastructure on premise. Why not put that in the cloud and refocus IT resources on more of the business innovation?

David Starr: Many health organizations can be reluctant to move to the cloud still, so what are some of their primary concerns?

David Houlding: Healthcare is facing incredible change on an unprecedented level, right? And, so healthcare is trying to move to value based care, pay for performance. We've got the drive to improve patient outcomes. We've got increasing patient engagement and improving their experiences through patient portals and other techniques. We've got the need to improve the experience of healthcare professionals even, reducing burnout and so forth.

So, one of the other things with cloud computing is it really enables healthcare to not only reduce cost but also by focusing resources on business innovation rather than low level on premise infrastructure, it paves the way for new levels of innovation and ability to adapt to new technologies including artificial intelligence, machine learning. We've got internet of medical things. We've got augmented reality, mixed reality, virtual reality, 5G and so forth.So, there's all these phenomenally exciting technologies that can help healthcare improve outcomes and engagement and all those good things, and cloud really helps provide the agility for healthcare to do that adaptation and evolution.

David Starr: Normally, when we talk about AI in healthcare, we talk about imagining or diagnostic imaging and all sorts of other really exotic uses of AI. This is simply using AI and machine learning capabilities to make my organization run more efficiently, and regardless of the fact that I'm a hospital or what have you. Is that right?

David Houlding: Yeah, absolutely, so there's the technologies and then the data. That's one of the key ones, diagnostic imaging, genomic, etc., and internet of medical things is another one, but it's really about how do we use the technologies, so how do we use the data to help healthcare meet the business needs and the business goals, and those are much more around what we call a quadruple aim, which is improving the outcomes of patients, improving the engagement and experience of patients, again, improving the experience of healthcare professionals, and of course reducing healthcare costs, so how can we use that data and those technologies and cloud computing to enable and empower healthcare to achieve those business goals?

David Starr: When a healthcare organization does decide to move to the cloud, what sort of things might they have struggles or might they have challenges with?

David Houlding: There was a really interesting study that Frost and Sullivan put out, the Healthcare Cloud Computing Hot Book, which was globally focused, looking at 2016 through 2021, and they looked at the top three criteria for cloud vendor selection. The top three were security; 41% of respondents indicated that as the top. That was the top concern overall, which is really interesting because maybe five years ago, a lot of healthcare was skeptical about cloud, looking at cloud as more risky, but today, a lot of healthcare views cloud as more secure than having on premise. The reality is healthcare doesn't necessarily have the deep security expertise to adequately secure on premise infrastructure, and so moving to cloud might be actually a much more secure option for many healthcare organizations, but nevertheless, security remains the top criteria for cloud vendor selection.

Reliability is second, up at 39%, and this is about as healthcare is moving, mission critical services, solutions, and systems, and data to the cloud. Are they going to be available, 24 by seven by 365? Also, even during the migration, right? If I migrate data or solutions to the cloud, are they gonna be available to me during that migration, or am I gonna have days of innovatability?

David Starr: [crosstalk 00:06:18] kinda got to change the tire while the car is moving.

David Houlding: Yeah, or operate on the patient. You gotta keep them alive, so those are great metaphors, but reliability is paramount. A lot of people equate security to just protecting confidentiality and preventing breeches, and that's a hugely important thing, but if there's anything that ransomware has taught us, protecting availability and ensuring reliable and access data and systems is as important if not more important. If healthcare is cut off from access to data or systems, it could be immediately disruptive, especially to healthcare providers, or any disruption like that could degrade or degrade service for sure, but potentially even increase patient risk. When an organization does decide to move into the cloud, what are some of the first things they're going to look at doing? We have a lot of different ways to get started in Azure. Maybe I'm moving data; maybe I'm just moving virtual machines. What do you find is the first step for most healthcare orgs?

Yeah, one of the first things to consider in moving to the cloud is how to get effective security and compliance, and one of the really important things to take away from this is there's a few key points. This is one of them. Security and compliance are a shared responsibility. It's not something you buy from a cloud provider. The division of responsibilities really depends on how healthcare is gonna use the cloud. If healthcare is using the cloud for infrastructure as a service, then they are responsible for certain things like the healthcare organization would still be responsible for data classification and accountability and client and endpoint protection, identity and access management, application of all controls, but then the cloud provider would help with network controls and host infrastructure and of course physical security, but as healthcare moves toward software as a service, more and more of those responsibilities fall on the cloud provider.

So, what's really important is it's not like healthcare goes out and purchases cloud and they're done with security and compliance, right? To get effective security and compliance, you have to have this wholistic picture of your security and compliance requirements. What are you getting from the cloud provider? What are you responsible for? And, it's really a partnership with your cloud provider to ensure that all of those requirements are met. Nothing falls through, and that's why Microsoft has really focused on not only provided highly secure platforms and tools but also a partnership with healthcare organizations to ensure that effective security and compliance.

Now, David, back to your question, in terms of how does healthcare move to the cloud, I think of it as a three step. There's really the enablement. Does the healthcare organization have the yes decision internally to move to the cloud? If they're not moving cloud already. If they are using cloud already, do they have a yes decision internally to expand their use of cloud? And, oftentimes, if they do not have a yes decision internally, it's because of residual concerns, many of which center around security and reliability. So, getting to that yes decision is a critical step. Yes, we can move to the cloud. We can start using cloud, or we can expand use of cloud. The second step in healthcare moving to the cloud is really landing in the cloud. Initially, a lot of healthcare organizations will use the cloud for pretty basic used cases like data management, storage and archiving, backup and restore, business continuity, disaster recovery, just secure and reliable management of data in the cloud.

Another sort of initial use case in the cloud is software as a service, and this is healthcare moving their block and tackle enterprise systems to the cloud, could be an electronic health record system or electronic medical record system. It could be a payer system to manage claims and membership and eligibility and due adjudication, all that good stuff, any kind of basic records management system hosted in the cloud and provided as software as a service to healthcare is gonna free healthcare up from maintaining that low level infrastructure and enable them to focus more on business innovation.

The third step in the sort of journey to cloud is really once you've the yes decision, you're doing the data management. You're doing the software as a service, really growing the use of cloud around strategic new technologies like analytics, AI, machine learning, internet of medical things, powering those with new data. We've got augmented reality and all those exciting things. And, cloud is poised to really enable those, but that's how I think of healthcare moving to the cloud. Now, of course, again, security and reliability are key to the enablement and getting the yes decision.

David Starr: [crosstalk 00:11:30] You sort of start there right in your design?

David Houlding: Absolutely, and then beyond that, maintaining the security and compliance on an ongoing basis is essential, right? To enable healthcare to meet the businesses goals while mitigating things like ransomware, denial of service tax, breeches, etc. So, security and compliance are not a one and done point in time check the box, move on type of thing. It's an ongoing thing, right? You've gotta make sure you have effective security all the time on an ongoing basis. Otherwise, you're at risk of these other kinds of security incidents.

David Starr: So, with that in mind, what does Azure specifically do for the concerns of security, privacy, reliance, these sorts of things?

David Houlding: Yeah, so security, any security professional will break down security into what we call CIA, confidentiality, integrity, and availability. And, on the confidentiality side, we're really talking about ensuring only authorized access to sensitive healthcare data, and that's done with access controls, like role based access control in Azure, multi-factor authentication, encryption of data in Azure, rest and in transit, key management with the Azure key vault and so forth.

Now, on the integrity side, ensuring data is accurate, complete, and up to data, audit logging, who did what, when, why, etc., hash codes and digital signatures to enable the authenticity to be verified and easy detection of tampering. That's all to protect the integrity of systems in data, and then on the availabilities side, ensuring timely and reliable access to systems and data, we've got Azure back up and restore, which can work on virtual machines. We've got Azure's site recovery, service for business continuity, and disaster recovery, and you can have redundancy across availability zones. You can upload balancing automated fail over. Azure has a huge worldwide footprint. We've got 54 regions serving I think 140 countries at present, but also that's protections like ... D DoS protection or distributed deny them service protection. There's Azure D DoS protection services, and so again, CIA, protecting confidentiality, integrity, and availability, and that kinda breaks it down and gives you a sampling of Azure's services, things that are embedded in the platform and the tools available.

But, the other thing to think about in the availability area is reliability. Again it's migrating to the cloud without disruption. There are a lot of Microsoft partners out there that specialize in helping healthcare identify suitable solutions to move to cloud and helping them migrate those solutions to cloud in a seamless way that they don't have any disruption in availability, and then reliability is also of course maintaining business continuity on an ongoing basis, again, incredibly important especially for systems that used by healthcare providers where if there's any disruption to those systems, it could degrade healthcare, even be a patient safety risk. If the patient goes to a doctor, a hospital, and their records are unavailable, that's a major issue, not just an inconvenience. It could be a patient's safety issue.

There's ongoing threat detection because new threats are emerging all the time, new vulnerabilities. We've got intelligence security graph at Microsoft, which is really an advanced analytics service that links massive amounts of threat intelligence and security data to provide unparalleled threat detection and protection. We've got the Azure security center, a unified view of security both on premise and in the cloud. You could have Azure's stock on premise, and you could be using the Azure cloud, and that's gonna really provide 24/7 security monitoring to protect your application and assets and data. And, so the Azure security center enables the management of alerts and vulnerabilities. It's a single dashboard. There's integration with sim tools, security information, and event management, so you can integrate with sim tools again for a single dashboard.

Now, for compliance, the key questions are really what kinds of data you're dealing with, what kinds of sensitive data, right, and PII or personally identifiable information is really key. What kinds of data are you dealing with? It can locate, be used to contact, or be used to identify a patient. That's PII, and then any healthcare data associated with a PII is often called PHI, or protected healthcare information, and when you're dealing with PII or PHI, that's gonna determine to some extent what laws and regulations apply. If you're in the US, you're dealing with healthcare data PHI. You're gonna be concerned about HIPA. If you're using European citizen data, you may be impacted by GDPR.

So, there's the type of data you're dealing with. There's also where is the data located? So, you need to think about not just the cloud as some sort of abstract but where the actual data centers that you're using are physically located because that can determine in some cases the jurisdictions, what regulations and data protection laws apply will depend on where you're putting that data. So, Azure has a huge set of compliance certifications. I believe the most certifications of any cloud platform, those obviously include HIPA, High Trust, GDPR, ISA 2700 Series. You've got PCIDSS and many more, David, that we might be able to provide a link in the podcast text because there's just such a huge array that people can look at.

David Starr: We'll include a link to the industry certifications and compliance page. You can actually look up the certifications that Azure adheres to based on industry.

David Houlding: Yeah, good point, absolutely. That's a great next step because a lot of folks will have particular ones in mind, and they'll be interested in does it support those. The way to think about these is not just if I get this or that cloud, will I get HIPA. Again, that's a shared responsibility model, so HIPA certification will show you that Azure provides platform and associated tools, and there's partnership from Microsoft to help you achieve HIPA compliance. Ultimately, the healthcare organization that cover identity or business associate is what's held to HIPA compliance, not any particular tool or platform, and Microsoft tools and platforms are certified to enable healthcare organizations to achieve compliance. That's an important distinction, but there's the Azure compliance manager. This is a tool, a dashboard, that can really map technology solutions to regulatory requirements, data protection laws, etc., security standards, and enable a management of action items and workflow to ensure remediation of any non-compliance items, so the healthcare organization using Azure can go into the compliance manager, indicate, okay I need to comply with HIPA; I need to comply with GDPR, and it'll show them how those relate to the Azure platform and tools, any sort of remediation gaps or non-compliance gaps rather will emerge from the dashboard. The compliance manager provides the sort of action item capability, the assignment capability, and the workflow capability to enable you to manage the remediation of any non-compliance items.

That's super important because you don't want anything to fall through the cracks, especially when they're shared responsibility, and the other thing is just like security, compliance is not a one and done thing. It's an ongoing thing, right? And, things are always changing. You might be expanding your sub cloud. There's new technologies emerging, etc., regulations and data protection laws are changing over time, and so the compliance manager will track compliance on an ongoing basis to ensure that any new non-compliance items that emerge over time will be raised as alerts, and then you can kick off remediation to assure again that you have full compliance over the long term.

David Starr: That's a fantastic service built right into Azure. Shifting gears, how do customers get to partner solutions? Because, Microsoft is rather unique, right, we don't build the solutions themselves necessarily, but we build the infrastructure, and then we have a set of partners that come in and build in solutions on top of that, so how do customers get to those partner solutions?

David Houlding: Yeah, great question. There's just so many partners out there that provide solutions and/or services to help healthcare move to the cloud including managing security and compliance and reliability and all those things, but one of the best places to go is the Azure marketplace. If you visit the Azure marketplace, you can see the current set of solutions and services available to help you move to the cloud, maximize your use of the cloud, and that's changing over time, so visit back regularly.

The other opportunity out here is if you are an organization that helps healthcare organizations with solutions or services to move to the cloud, there may be opportunities for you to publish your services and or your solutions in the Azure marketplace, so we'll invite you to reach out to us. You can reach out to me on LinkedIn. David, I think we can include a link in the podcast, post as well, so people know where to connect if they're interested.

David Starr: Absolutely, those links, we'll include in the show notes. I'll also note that in the show notes, we will link directly to the use case that underlies the conversation we're having here on the show today.

David Houlding: Perfect.

David Starr: I think we're about at the end of our time, David. I can't tell you how much I appreciate you being on the show today.

David Houlding: It's been great, David. Thanks very much for the opportunity.

David Starr: Thank you for joining us for this episode of the Microsoft Industry Experience's team podcast, the show that explores how industry experts are transforming businesses with Azure. Visit our team at aka.ms/indexp, and don't forget to join us for our next episode.