PHI and the Cloud: Caveat Emptor

Kurt Hagerman
Chief Information Security Officer

HITRUST 2014
24 April, 2014
Cloud Peace of Mind

What did you consider when looking to leverage the cloud for PHI?

- Security
- Availability / Agility
- Performance
- How it impacts my HIPAA compliance
- Service
Did you find it?
(If not it’s understandable given the messaging you’re seeing)
Here’s What They’re Saying…

**Guaranteed HIPAA Compliant Hosting & Managed Services**

No matter what your role is with patient protected health information (PHI), all the other vendors that you work with are relying on you to do your part in compliance. When you work with [payer networks, ISVs, or other entities that store, transmit or process PHI data](#) – that you are **100% HIPAA compliant – guaranteed**. With this kind of compliance guarantee, your value as a trusted partner will increase, improving your credibility and opening the door to more revenue opportunities.

Don’t settle for HIPAA-ready - invest in a HIPAA compliant cloud that has been independently audited and found to be **100% HIPAA compliant**.

**Leave the HIPAA compliance to us**

HIPAA compliant hosting services can relieve you of the complex demands of compliance. With our solution, each key HIPAA mandate is met, ensuring that your sensitive patient information is fully secure and that you’ll pass every HIPAA-related audit.

**HIPAA Compliant Hosting**

We passed an independent HIPAA audit with **100% compliance** against the new OCR HIPAA Audit Protocol. Our **encrypted HIPAA cloud** offers protection of data at rest & in transit.
Here’s More of What They’re Saying…

100% HIPAA Compliant & Business Associates Agreement (BAA) Friendly:

Our world-class data centers and HIPAA Compliant Managed Hosting Services successfully undergo independent 3rd party HIPAA assessments to demonstrate our 100% HIPAA compliance, allowing our many healthcare and dental customers to satisfy their HIPAA security obligations. We are also Business Associates Agreement (BAA) friendly, and we routinely enter into Business Associates Agreements with our customers.
Are you confused, frustrated (I know I am)?

- I think you’ll agree that these are pretty outrageous statements being made.
- They sound good but remind me of the old Wendy’s commercial where Clara shouts out “Where’s the beef?”
- What do they actually mean to you, the cloud consumer?

**Question for the audience:** “How easy is/was it for you to get past the hype and figure out what they are actually going to do for you?”
Trivializing HIPAA Compliance

• There is no Easy Button
• Vendors over simplify the requirements to sell their services as a silver bullet – snake oil anyone?
• HIPAA is risk based for a reason
It’s Not What They Say…
It’s What They **DO**

- Do you know what your vendor is really doing for you?
- Do they provide information on the specific security controls that are included with their service?
- Have they mapped their services and security controls to the HIPAA/HITECH requirements?
- Does your vendor use third parties to provide services to you?
- Have they (and their third parties) been independently assessed?
- Do you know who to call when something goes wrong?
- What about the privacy and breach rule?
- How do I manage a compliance program with multiple vendors all providing my “cloud services”?
Be A Smarter Cloud Consumer

You need to deal with vendors who will be transparent about how what they do directly assists you in mitigating risk and addressing your compliance requirements.

Your vendor should……..

• Provide a clear concise explanation of the specific security controls they include and how these assist you

• Be able to articulate the boundaries between their responsibility and yours

• Provide you with documentation that backs up any assertions they make about being “HIPAA Compliant” including independent audit reports that clearly state the scope of the assessment, the controls framework used and especially how this compliance can be leveraged by YOU
Be A Smarter Cloud Consumer

**What about Business Associate Agreements?**

Many vendors say they are “business associate friendly” and that they will sign a BAA.

**Does their BAA include language that clearly states what services they are providing?**

**Do they suggest this language when reviewing yours?**

Your vendor should……..

- **Demonstrate that they understand the requirements that they are subject to**
- **Engage in a meaningful conversation around the division of responsibilities and suggest/include this in your BAA**
So Far We’ve Talked About Security and Compliance

You have Business Critical applications that need to provide access to data NOW to ensure the quality of patient care

So What About Performance and Availability?
Performance and Availability

The nature of healthcare information requires that it be available without delay when it’s needed

- Lots of focus on IOPS but that's not the whole story
- Latency between the application and storage is a better measure
- Not all storage is created equal
- Fast is great but what about security of your data?

Availability of PHI is a core requirement of HIPAA

- How do you ensure resiliency and redundancy?
- Not all storage is by default highly available
Performance and Availability
(What to ask your vendor)

• What type of storage do they provide?
• Are there multiple tiers / options?
• SSD is becoming more popular but your mileage may vary – find out who their vendor is and research them
• Don’t just take IOPS numbers / guarantees – ask about latency
• How is it connected / presented to your server?
• How do they ensure segmentation between customers?
• What is their data destruction process?
• Do they provide high availability by default or is this extra (if it’s even available)? If so, how?
• Ask for a POC environment so you can test your applications and judge for your self
Using “the Cloud” for PHI is Possible

Caveat Emptor – be a smart cloud consumer

Find vendors who...

- Provide detailed information about their security and how it matters to you
- Provide meaningful documentation backing up their claims around HIPAA compliance
- Will engage in serious conversation about how what they do will make your compliance process easier
- Will address your performance requirements and are willing to let you “try before you buy”
Questions?
Thank You

Kurt Hagerman
Chief Information Security Officer

Email: kurt.hagerman@firehost.com
Phone: 877.262.3473 x8073