WEDI Strategic National Implementation Process (SNIP)
Privacy & Security Workgroup
Cloud Computing Sub-workgroup

Cloud Computing White Paper

USING PHI & CLOUD COMPUTING: A FOCUS ON THE INTERSECTION OF CLOUD TECHNOLOGY AND PRIVACY/SECURITY

July 2012

Workgroup for Electronic Data Interchange
1984 Isaac Newton Square, Suite 304, Reston, VA. 20190
T: 202-684-7794//F: 202-318-4812

CONTENTS

Disclaimer

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the WEDI Strategic National Implementation Process (WEDI SNIP).

Document is for Education and Awareness Use Only

White Paper – Using PHI & Cloud Computing: A Focus on the Intersection of Cloud Technology and HIPAA/HITECH Privacy & Security

I. Purpose

This white paper has been created to focus on the intersection of cloud technology and HIPAA/HITECH Privacy and Security requirements. It is recognized that many resources are available on both topics. However, it appears that little information is yet available on the intersection of the two.

II. Scope

The Workgroup for Electronic Data Interchange (WEDI) Strategic National Implementation Process (SNIP) Privacy & Security Cloud Computing Sub-Workgroup was created in order to offer industry guidance and practical information on the use of this new and exciting technology environment as it relates specifically to healthcare data.

The Cloud Computing Sub-Workgroup first gathered in early 2012 and reviewed its charter, which included the responsibility to offer the healthcare industry tools/white papers and other informative materials. A cross representation of industries participated, including but not limited to representation by individuals with in-depth experience of privacy and security requirements, data handling, and cloud computing technologies.

Upon initial discussion it was acknowledged that there are a number of resources available for learning about cloud technologies as well as many that provide guidance on privacy and security. However, little information is currently available on the intersection between these two areas. Additionally, when formulating a case study, it was found that participants had varied ideas of what the cloud was and what specific functionality it should have in order to safeguard and protect PHI (Protected Health Information).

Therefore, it was decided that the most prudent place to begin our work was to conduct a survey on the industry's definition and uses of cloud computing. This would give the group the opportunity to ask more specific questions across a number of companies and accrediting bodies and then compile them into one document.

Questions were submitted by participants of the sub-workgroup and then compiled into a logical order. Participants were then challenged to identify organizations to complete and submit responses. Once received and compiled, the responses would begin to "tell the story" of where our industry currently stands with respect to the use of cloud computing to secure and protect sensitive health information.

III. About the Cloud…

Privacy and Security Concerns about Cloud Computing. For some organizations, just mentioning the words "sensitive health information" and "cloud" in the same sentence brings on fear, uncertainty and doubt. In particular, HIPAA covered entities and business associates may worry about potential breach situations due to multiple organizations sharing the same networks and/or processors; administration and handling by third parties (which hand off to third parties which hand off to third parties). This white paper only begins the process of showing the benefits and challenges associated with our health care industry's use of cloud technology. Additional, more in-depth white papers will follow. For this edition, we have begun the discussion by focusing on some of the benefits.

Recovery and Security Benefits of Cloud Computing. Cloud computing represents the new frontier in data storage. It has been adopted by many industries due to its high level of efficiency and security as compared with traditional data storage methods. Due to its cost-effective nature and its adaptability to specialized uses and data formats many industries, including the health care industry, have started to take an interest in cloud computing as their primary means of data storage. Cloud computing is based on the virtualization of data, which eliminates the need for local server farms that are vulnerable to un-recoverable damage or breach. Cloud computing provides several benefits that traditional data storage lacks. These benefits are most easily recognizable in two areas:

1. Disaster Recovery

   In terms of disaster recovery, cloud computing delivers faster recovery time. Because cloud computing is based on virtualization of data, "the entire server, including the operating system, applications, patches and data is encapsulated into a single software bundle or virtual server. This entire virtual server can be copied or backed up to an offsite data center and spun up on a virtual host in a matter of minutes."[1] Because the virtual server is independent of hardware, the operating system, applications, and data can be *safely* and accurately transferred from one data center to another without the burden of physically reloading each component of the server. This is a much faster and cost-effective process than

[1] "Benefits of Disaster Recovery in Cloud Computing," http://www.onlinetech.com/resources/e-tips/disaster-recovery/benefits-of-disaster-recovery-in-cloud-computing

replacing or recovering data from crashed or damaged servers. The recovery speed of online, offsite backups through cloud computing makes it difficult to justify older, slower, and less precise methods of data storage and recovery. An added benefit of disaster recovery with cloud computing is "the ability to finely tune the costs and performance for the Disaster Recovery (DR) platform. Applications and servers that are deemed less critical in a disaster can be tuned down with less resources, while assuring that the most critical applications get the resources they need to keep the business running through the disaster."[2] Cloud disaster recovery improves Recovery Time Objectives (RTO) and can be secured with encryption, logging vulnerability and penetration testing to ensure that the data is secure and safely backed-up.

2. Security Breach

Elimination of physical data theft—in the last few years the theft of PHI, especially in the health care industry, has dominated the news. In 2011, 4.9 million people were affected by the TRICARE data breach, where data backup tapes were physically stolen. A TRICARE contractor and business associate that provided offsite backup, storage and data security for TRICARE, was found responsible after it was discovered that the data backup tapes were taken from the back of an employee's car.[3] The contractor was sued in a class action lawsuit by those affected by the breach, who sought $1,000 in damages for each affected individual. Physical theft is one of the most common forms of HIPAA breaches, and traditional data storage methods on tapes and other tangible formats make physical theft much easier to accomplish. The virtualization of cloud computing can eliminate the possibility of physical data theft, and increases the security of PHI and HIPAA-sensitive information.

Cloud computing allows for the control that HIPAA-sensitive organizations require over their data. Private cloud computing dedicates exclusive hardware to each user, which maintains the privacy of protected health information and prevents accidental or purposeful access by outside entities. Furthermore, cloud computing is flexible enough to allow for re-allocation of resources and re-sizing of a server with ease, which prevents periods of time when PHI is not secured on a server because the user underestimated the disk space or RAM needed to hold data. Incredible redundancy can also be achieved by connecting to a private Cloud, and the ability to shift the data seamlessly between server resources

---

[2] Id.

[3] Pham, Thu. "Military Healthcare Contractor's HIPAA Breach Followed by $4.9 Billion Lawsuit," OTBlog, Published October 18, 2011. http://resource.onlinetech.com/military-healthcare-contractor%E2%80%99s-hipaa-breach-followed-by-4-9-billion-lawsuit/

allows for maintenance or re-design/re-sizing without incurring unwanted downtime.[4]

IV. About Privacy and Security

As mentioned above, *HIPAA-sensitive* organizations must implement specific controls over how data they are responsible for is handled – including when leveraging cloud technology. When considering the privacy and security elements necessary to protect PHI, HIPAA covered entities or business associates should begin by conducting a HIPAA required Risk Analysis.

The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

NOTE: This is currently a requirement of HIPAA Covered Entities; will be a required element for Business Associates (HITECH); and, is a component of Meaningful Use for providers applying for EHR funding from CMS.

The process of risk analysis may be very different from organization to organization. However, in order to conduct a comprehensive assessment, the organization must first begin by understanding the data it is charged to protect. WEDI SNIP Privacy & Security has called that process "conducting a PHI Flow". This may be completed on a spreadsheet or other simple manner. But whether using a very complex method (tool/technology) or a simple spreadsheet the goal is the same: understand how the organization creates, receives, maintains and transmits PHI and document such. After this first step, a process can be taken to examine and take steps to reduce potential risks to such data. Risk analysis may include but not be limited to technical penetration assessments, review of policy controls, interviews with staff, forms of assessing threat impacts and likelihood etc… But, however one undergoes this process, it should be an ongoing function and must result in mitigation of identified issues.

The WEDI SNIP S&P Cloud Sub-workgroup expects that the implementation of Cloud computing by a HIPAA/HITECH affected organization subject to HIPAA/HITECH will trigger further risk analysis efforts as defined below.

Excerpts from the Office for Civil Rights Guidance on Conducting A Risk Analysis (2010) are as follows:

Scope of the Analysis

---

[4] "Top 5 Reasons Why Yout Company Should Transition to Private Cloud Computing," http://www.onlinetech.com/resources/e-tips/cloud-computing/top-5-reasons-why-your-company-should-transition-to-private-cloud-computing

The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization **creates, receives, maintains, or transmits**. (45 C.F.R. § 164.306(a).) This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. Thus, an organization's risk analysis should take into account all of its e-PHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its e-PHI.

Data Collection

An organization must identify where the e-PHI is stored, received, maintained or transmitted. An organization could gather relevant data by reviewing past and/or existing projects, performing interviews, reviewing documentation, or using other data gathering techniques. The data on e-PHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)

Identify and Document Potential Threats and Vulnerabilities

Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii).) Organizations may identify different threats that are unique to the circumstances of their environment. Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Assess Current Security Measures

Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

The security measures implemented to reduce risk will vary among organizations. For example, small organizations tend to have more control within their environment. Small organizations also tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard e-PHI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of e-PHI in a small organization may differ from those that are appropriate in large organizations.[5]

Determine the Likelihood of Threat Occurrence

[5] HIPAA Security Standards: Guidance on Risk Analysis, Office of Civil Rights (OCR) 5/7/2010. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf.

NOTE: This is also the area of the process where an organization should determine if additional information can be further secured by invoking encryption controls in an effort to reduce the risk of data breaches.

The Security Rule requires organizations to take into account the probability of potential risks to e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires protection against because they are "reasonably anticipated."

The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of e-PHI of an organization. (See 45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

Determine the Potential Impact of Threat Occurrence

The Rule also requires consideration of the "criticality," or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) An organization must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.

The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e-PHI within an organization. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

Determine the Level of Risk

Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

Finalize Documentation

The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).) The risk analysis documentation is a direct input to the risk management process.

Periodic Review and Updates to the Risk Assessment

The risk analysis process should be ongoing. In order for an entity to update and document its security measures "as needed," which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).) The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. For example, if the covered entity has experienced a security incident, has had change in ownership, turnover in key staff or management, is planning to incorporate new technology to make operations more efficient, the potential risk of the change should be analyzed to ensure the e-PHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the evolving threats or vulnerabilities, a changing business environment, or the introduction of new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and adjusting risk management processes to address risks in a timely manner will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

V. Survey Responses

As was mentioned in the Scope Section of this document, the Cloud Computing Sub-Workgroup created a Cloud Computing Survey and solicited responses from ten (10) organizations representing a cross section of classifications. Five (5) of the ten organizations contacted responded with completed surveys. The responding organizations represent a wide range of classifications:

- Vendor (3)
- State agency client (1)
- Accrediting organization (1)

All of those contacted currently use or sell (or accredit organizations that use or sell) cloud computing services located in the United States. The key survey finding is that all respondents ensure privacy/security of protected health information and other sensitive information with use of cloud computing in several ways including:

- data encryption
- privacy/security policies, procedures, and training programs
- HIPAA/ HITECH compliant business associate (BA) agreements

More detailed responses are included in Appendix B, Table 1. It is important to note that due to the small sample size, this survey outreach was simply a poll and not meant to be generalizable. However, the responses are very useful in gaining an overall sense of where the current healthcare industry is positioned regarding the use of cloud

computing environments for healthcare data. This general information “sets the stage” for more in-depth work by the WEDI SNIP Privacy and Security Cloud Sub-workgroup.

VI. Summary

While flawless security may never be achieved, Cloud computing represents the next step in data security, and has proven to be a worthwhile investment to many industries. The nature of its design increases accurate and secure disaster recovery, and provides notable protection against physical theft. The healthcare industry should benefit from the advantages provided by Cloud computing due to the highly-sensitive nature of the PHI that it is responsible for safeguarding. While Cloud computing is a developing field in data security and storage, it provides an excellent insight into the future of health information technology.

The WEDI SNIP S&P Cloud Sub-workgroup hopes this document provides an early look into the ways organizations are leveraging cloud technology while safeguarding and protecting Protected Health Information.

VII. Acknowledgements

Don Bechtel	Siemens; Chairman, WEDI Board of Directors
Lesley Berkeyheiser	Principal, The Clayton Group, LLC; Co-Chair, WEDI SNIP Security & Privacy Workgroup Co-Chair
Chris Bowen	ClearData.net
Mark Cone	Principal, N-Tegrity Solutions Group; WEDI SNIP Privacy & Security Workgroup Co-Chair
Rachel Devoto, J.D.	Process Consultant for Acquisitions at Humana Inc.
David Ginsberg	PrivaPlan Associates; WEDI SNIP Privacy & Security Workgroup Co-Chair
Lori Hale	Senior Business Consultant, Michigan Public Health Institute
Suzanne Jones	Principal, WriteMode; Technical Writer, N-Tegrity Solutions Group
Lola Jordan	CDS
Sue Miller	Principal, Susan A. Miller, J.D.; WEDI SNIP Privacy & Security Workgroup Co-Chair
Ron Moser	Moserhaus Consulting; EHNAC

Appendices

Appendix A - References

DRAFT Cloud Computing Synopsis and Recommendations

HIPAA Security Standards: Guidance on Risk Analysis, Office of Civil Rights (OCR) 5/7/2010. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf.

NIST Special Publication 800-146

Risk Management Guide for Information Technology: Systems Recommendations of the National Institute of Standards and Technology. (*For characteristics, definitions and service models*) http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

Appendix B – Cloud Computing Survey (Response Summary)

Note: Due to the small sample size, this survey outreach was simply a poll and not meant to be generalizable. However, the responses are very useful in gaining an overall sense of where the current healthcare industry is positioned regarding the use of cloud computing environments for healthcare data. This general information "sets the stage" for more in-depth work by the WEDI SNIP Privacy and Security Cloud Sub-workgroup.

1.	**Do you currently use a cloud computing service?**	Yes-5
2.	**What elements of protected health information (PHI) and other sensitive information are going into the cloud?** *Individual data (patient/member data (depends upon full hosting or part of data back up as Disaster Recovery Plan). May include "full chart" such as complete medical records, (demographic, clinical and financial data) in support of such functions as patient care, research, and marketing. All respondents noted the usage for this type of data is in a Private Cloud (not Public).*	*(See response summary below question at left.)*
3.	**What kind of a cloud is being used?** *Private Clouds were clearly preferred if not required across respondents. An auditable "chain of trust" between the parties handling the data in the Cloud was also preferred. The most referenced architecture type is "Infrastructure As A Service" or IaaS.*	*(See response summary below question at left.)*
3.a.	**Is the data encrypted? When is it encrypted? (In transition; rest; use)**	Yes-3 Yes and No – 1 N/A-1
3.b.	**Is it a public or a private cloud or a hybrid?**	Private-1 Hybrid –1 Combo-2 N/A-1
3.c.	**Are you hosting it within your IT department or through another vendor?**	IT Dept – 2 Another vendor-1 N/A – 2

4.	**Who is able to access the data stored in the cloud, and how is the data accessible?** *Respondents overwhelming referenced the use of Role Based Access to allow for the "customer" to have access (customer may be but is not limited to a Provider Hospital or Clinic; Patient; or Data Sender). Most respondents also referenced that the person assigned as the Storage Administrator and Application Vendor/full hosting was also frequently mentioned as having access for support purposes. The most mentioned method for access referred to for technical safeguards was the use of secure VPN channels.*	*(See response summary below question at left.)*
5.	**What limits are placed on the cloud in terms of use of the data for non-storage purposes? For example, is the cloud computing vendor able to use the patient data for non-healthcare purposes such as advertisement?** *The majority of respondents stated that the Cloud vendor was not provided access at all to the data (and the data is encrypted). Some allowed access for maintenance purposes. No other uses were allowed (via contract).*	*(See response summary below question at left.)*
6.	**Is the data partitioned on the server?** **If so, how? (Name technology if known and whether by government? By private? Or by individual entity?)**	Yes -2 Yes and No– 2 N/A-1 • How? Ind.Ent-1 • How? Combo-1 • How? N/A-3
7.	**How is the data center secured? Physical and logical?** *All respondents indicated that multi-layers of physical and logical controls were used to secure the data center. Many cited levels such as Tier III DoD grade; HIPAA/NIST standards.*	*(See response summary below question at left.)*
8.	**Is the data center physically located within the U.S.?**	Yes-5
8.a.	**Can you identify every physical location housing the PHI?**	Yes-5
8.b.	**Is the cloud single vendor or multi-vendor?**	Single – 3 Both – 1 N/A-1
8.c.	**Are there privacy/security policies, procedures, and training programs in place at all locations (where PHI is handled via the cloud)?**	Yes-5
8.d.	**Do you understand the laws of the country hosting your PHI (and other sensitive information) in context of legal protection and cooperation with the U.S./with following U.S. and state laws?**	Yes–5

9.	**What type of data recovery capabilities is preferred for a cloud-computing environment?** *Responses included: Tiered approach; Redundancy; Automatic failover, up to and including backup Data Center. Specifics were driven by Service Level Agreements, but full data store within 48 hours or less was cited.*	*(See response summary below question at left.)*
10.	**What kind of contract is secured for all parties involved with the cloud-hosted data?** *Responses included; "normal business contracts; Service Level Agreements (SLA) ; Acceptable Use Agreements; Network Usage Policies, Business Associate Agreements (BAA) ; Master Service Agreements (MSA) and Statement's of Work (SOW).*	*(See response summary below question at left.)*
10.a.	**Is a HIPAA/ HITECH compliant business associate (BA) agreement in place for every party that can gain access to PHI including system administrators, data center vendors, etc.?**	Yes-5
10.b.	**Do you have a standard business associate agreement that must be used for all parties touching your data?**	Yes-4 Yes and No-1
10.c.	**What privacy and security training is required for vendors with access to PHI? (Other sensitive information?)** *Security awareness training; Routine reminders and detailed training on related policies and procedures were included in the responses.*	*(See response summary below question at left.)*
10.d.	**What kind of contract is secured for all parties involved with the cloud hosted data?** *Responses included; "normal business contracts; Service Level Agreements (SLA) ; Acceptable Use Agreements; Network Usage Policies, Business Associate Agreements (BAA) ; Master Service Agreements (MSA) and Statement's of Work (SOW).*	*(See response summary below question at left.)*
10.e.	**Do you review cloud computing company's privacy and security policies and procedures? If yes, when (prior to contracting or during a routine check?)**	Yes-3 N/A-2
10.f.	**What auditable processes are required for access?** *Processes to be considered for audit include: Multi-factor authentication; Unique user ID's;, Minimum Necessary Requirements; and Role Based Access*	*(See response summary below question at left.)*

11.	**Do you require your cloud vendor to document their risk assessments?**	Yes-3 N/A-2
11.a.	**Do you review such information?**	Yes-3 N/A-2
11.a.i.	**Do you follow-up to assure remediation activities (identified during the risk assessment) were carried out?**	Yes-3 N/A-2
12.	**Does your organization have any type of system characterization document(s) that define system boundaries; functions; data criticality?**	Yes-5
12.a.	**PHI flow?**	Yes-5
12.b.	**System architecture? Including description of servers and firewalls supporting your technical infrastructure?**	Yes-5
13.	**Has your workforce been through any education on HIPAA and organizational policies and procedures?**	Yes-5
13.a.	**Do you keep records of training and who attended?**	Yes-5
13.b.	**Does each workforce member attest to confidentiality requirements for data handled by the organization?**	Yes-5
14.	**Has your organization had any data breaches in the last 12 months? If yes, please explain.**	No–4 N/A-1
15.	**What type of security breaches in past performance do you review for your selected cloud vendor to ensure it is a trusted entity?** *None of the participants reported that this question was applicable to their organization.*	*(See response summary below question at left.)*

Table 1- Quantifiable Responses (Summary)