Private Information Protection in Cloud Computing – laws, Compliance and Cloud Security Misconceptions

Special research prepared by Rubos, Inc. team

(We do independent research on security matters in various domains)

Prepared for OWASP AppSec 2012

Presented by Mikhail Utin, CISSP, Ph.D.

(Questions will be answered after the presentation. Please, submit them to the speaker in writing.)

1. Introduction (1)

A bit of Cloud Computing (CC) history:

- Not new as a service, new concept of crossing legal borders
- CC security research started only in 2008 – 2009 ignoring legal side and concentrating on “data protection”
- No regulation – any security rules set by CC and a customer
- Personal Information (PI) protection: HIPAA/HITECH, SOX, GLBA, PCI DSS, MA MGL 93H/ 201 CMR 17.00, numerous federal documents, etc. require certain relationship between CC provider and a customer
- HIPAA is the most developed in identifying provider and customer relationship
- Laws dictate different approach to CC security analysis – how binding relationship could be made legal, and then followed by technical implementation.

1. Introduction (2) – Delegation of Trust

New concept – Delegation of Trust (DoT)- in terms of requiring appropriate relationship between PI owner and a service provider: the provider guarantees certain level of security, and customer delegates trust to the provider. Such process is outlined in HIPAA Security Rule (45CFR Part 164):

Paragraph 164.308(b)(1)“*...A covered entity in accordance with 164.306 may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity behalf only if the covered entity obtains satisfactory assurances in accordance with 164.314(a) that the business associate will appropriately safeguard the information*”.

1. Introduction (3) – important HIPAA quotes:

Contracts between covered entity and a business associate: Paragraph 164.314(2)(i):

- *"Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will -*
- *(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic protected health information that is creates, receives, maintains or transmits on behalf of the covered entity as required by this sub-part;"*

1. Introduction (4) – important HIPAA quotes:

- Once initial trust is established, DoT chain can expend further: Paragraph 164.314(2)(i)(B):
- *"Ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it."*.

Logical assumption: Each component of DoT chain should have equal or better safeguards than business associate.

1. Introduction (final)

- **The basis of DoT concept is knowing the entire chain of service providers, and security status of each chain component and then engage in binding relationship utilizing appropriate legal instruments.**
- Analysis of services provided by CC in the context of widely used Deployment and Services models - how they will be affected by above mentioned regulations
- Necessary binding agreements between PI owner and service provider, and certain security processes, and if and how such relationship could be implemented
- Finding a solution to the fundamental **legal** DoT problem, and then considering more specific security issues (10 or more of known)

2. What is Cloud Computing – an overview

"*... the delivery of computing as a service rather than a product...*" – Wikipedia

2.1. Short history of Cloud Computing and security concerns

- Back in time: Internet Bubble - 10% of hosting production capacity of **hosting services** were in use – Amazon.com - 2006 "Amazon Web Service" - first application CC
- Numerous CC service providers: moving data across legal and physical borders followed to Amazon initiative
- No security concerns until 2009: security related references in Wikipedia: 4 of 2009, 4 -2010, 3 -2011 of 77 total
- US Government created Cloud Security Group in 2009, and both NIST Cloud Computing publications [2, 3] went public in 2011

2.1 What is Cloud Computing - two conclusions:

- Cloud Computing was originated from the hosting service by extending its capabilities, and is a service by its nature; the infrastructure is irrelevant to its customers, and is only a medium to transfer and process data.
- Legal and security concerns have been largely ignored during the rapid development of CC technology up until 2009.

2.2. Cloud Computing is a Dynamic Hosting Service (1)

- “Computing” is a process of computation. Prominent examples are Analog Computing, Digital Computing, Mainframe Computing, and so on.
- A “cloud” itself cannot compute, and it is neither a method nor a means of computation. There is always a point (or resource) inside infrastructure, which at a given moment digitally compute
- Originally “Hosting Service”, **cloud is a service delivering data to a computational point and back to the user**.
- By its nature, CC is dynamic service moving computational point between various resources, and providing “dynamic” access to applications – either via API, or directly to an application itself

2.2. Cloud Computing is a Dynamic Hosting Service (2) - Cloud Computing Service Model

- So named “Platform as a Service – PaaS” is actually Application Programming Interface (API) to a Dynamic Hosting Service (DHS)
- So-called “Software as a Service – SaaS” is an Application Dynamic Hosting Service
- And - finally - “Infrastructure as a Service - IaaS” is a well-known Hosting Service; previously (as there were no other needs) hosting was for web sites only, and now it is left up to the infrastructure user how to use it and what to deploy it to.

2.3. Evolutionary vs. revolutionary names

- Dynamic Hosting service is correct and pure technical term and is “evolutionary” name
- Cloud Computing is pure marketing and “revolutionary” name
- Predecessor – “Intranet” web sites - Internet information resources - installed inside a company infrastructure, which all of sudden became “new” technology for upper management sale just by adding web sites for internal use
- - Navy and Marine Corp Intranet (NMCI) project is typical sales of multi-billion upgrade as new “concept”
- Now – “Cloud Computing” turn …

2.4. What is the Cloud Computing Deployment Model and do we really need it? (1)

Why do we need “Deployment Model” which is about **computing resources** and provides no explanation of how **data** moves inside or the exact meaning of service to the customer.

- The Public Cloud: “*...It is owned and operated by a cloud provider delivering cloud service to customers*”. Basically, “owned and operated by provider” implies Hosting Service infrastructure, or as we used to say “Hosting Service” or “Outsourced Hosting”. Basically, we are making a reference to a service again, meaning that there is supporting infrastructure. However, do we really need a new model of “Public Cloud” to explain what we know since year 2000 as “Hosting Service”?

2.4. What is the Cloud Computing Deployment Model and do we really need it? (2)

- Private Cloud [2] - *"... is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data center or outside of it."* If Private Cloud is comprised from customer's equipment – it is just well known "Local Network' or organization's "Wide Area Network". If two kind of networks – LAN and WAN – are operated by external entity, it is called "outsourcing". So, again we can easy explain new "Private Cloud" in old and easily understood terms – LAN, WAN, or Outsourced Infrastructure and such well established terms are much easier to comprehend and to use than "Private Cloud"

2.4. What is the Cloud Computing Deployment Model and do we really need it? (3)

- Community Cloud – [2]:*"...the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization."* This definition is vague in legal context. Hosting Service. If NIST is trying to explain that a "community" has only one agreement with a provider, then it is legally incorrect. A "community" is not a legal entity and cannot sign an agreement, unless organizations within form such entity legally. In this case, we again see one-to-one relationship, and "public cloud" – Hosting Service. So far, there is no legal practice of signing service agreement by a vague "community"

2.4. What is the Cloud Computing Deployment Model and do we really need it? (4)

- Finally “Hybrid Cloud” model: fundamentally, it is a composition – [2] “*...are more complex than the other deployment models, since they involve a composition of two or more clouds (private, community, or public). Each member remains a unique entity, but is bound to the others through standardized or proprietary technology that enables application and data portability among them.*” As far as services are concerned, this model is a composition of LAN/WAN (private cloud), and a hosting service (public cloud). “Community”, as we discussed above, is either a hosting service or cannot legally exist.

2.5. Cloud Computing models' research conclusion (1)

- Cloud Computing is a pure marketing term for extended hosting service
- Cloud Computing does not technically explain the nature of new service.
- "Dynamic Hosting Service" term is a better description, and does not require any new particular "scientific" models to explain it
- So named "Deployment Models" do not add to understanding of how exactly services are provided; LAN/WAN, hosting service, or infrastructure outsourcing would be more technically correct.

2.5. Cloud Computing models' research conclusion (2)

- There is no legal consideration in any of the Service or Deployment models. They do not define how customers and provider will legally operate. So named Service Agreement and Service Level Agreement set in NIST [2,3] are not considered in regulatory legal context at all.

3. Legal consideration of Dynamic Hosting Service (DHS, aka Cloud Computing) implementation (1)

- We see enormous marketing campaign to sell DHS/CC to HIPAA covered entities and other regulated industries without any serious consideration of its legal ground and technical implementation of regulations
- We have hundreds of thousands of covered entities in the US, and most of them are small and medium size businesses. They are easy targets who understand neither HIPAA Security Rule itself nor legal meaning and possibility of implementation of DHS/CC .

Legal consideration of Dynamic Hosting Service (DHS, aka Cloud Computing) implementation (2)

The Reality of CC Show:

- We have little doubt that our strictly technical DHS term will be happily ignored and never used by the service providers and even their customers. However, for clarity of this presentation, we will use it while identifying legal inconsistency problems and finding a better resolution.
- **Nevertheless - we continue:**

3.1. Anatomy of HIPAA Security Rule Part 164.308(b)(1) and 164.314(2) - (1)

Base on the HIPAA quote provided in Introduction “Business associate contracts and other arrangements”:

- Two parties (not “communities”) involved, which are named “covered entity” and “business associate”
- A contract is required, which is usually named as Business Associate Agreement (BAA)
- Covered entity explicitly permits operations on Electronic Protected Health Information (EPHI)
- Operations include: create, receive, maintain, or transmit
- Covered entity is responsible for obtaining “satisfactory assurance” from business associates concerning safeguarding EPHI

3.1. Anatomy of HIPAA Security Rule Part 164.308(b)(1) and 164.314(2) - (2)

Standard refers to 164.314(a) and to 164.314(a)(2)(i) "Business Associate contracts" requiring:

- (A) Implement administrative, physical and technical safeguards reasonably and appropriately to protect the confidentiality, integrity and availability of EPHI
- (B) Ensure that **any agent**, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it.

3.2. Implementation of DoT in contracts between a covered entity, providers and subcontractors (1)

According to DoT concept should be identified who provides services and what is security level of each.

Two options of legally providing such assurance:

- Business associate collects all security level guaranteeing agreements from sub-contractors and verification of security status documents as well.
- Business associate has legal agreement with other cloud providers representing them as one legal entity and thus will provide covered entity with one security guarantee agreement and one security status document.

3.2. Implementation of DoT in contracts between a covered entity, providers and subcontractors (2)

- **If all cloud providers** have the same capability of being active providers, i.e. **having customers**, then **each of them should possess corresponding agreements and security status documents for each of customers**
- **Customers regulated by other** laws (SOX, GLBA, etc.) or standards (like PCI DSS), which **will require the cloud to have appropriate legal assurance** (i.e. documents) **according to their regulations**.
- The cloud very likely has **non-regulated customers**, who would **prefer** some **simplified security rules to get less expensive service**

Thus, providers are required having very complex legal support of services.

There is no introduced by government unified security controls providing "military" grade security assurance.

3.2. Implementation of DoT in contracts between a covered entity, providers and subcontractors (3)

Compliance with HIPAA:

- Compliance status is to be identified by government audit only
- Neither software vendors nor cloud providers (business associates and sub-contractors) can claim as “compliant” - government audits covered entities only
- Business associates and sub-contractors can be audited by commercial auditors for “satisfactory assurance”, i.e. having security controls
- Possible source of “check list “ is DHHS/CMS Sample – Interview and Document Request [4]
- the implications of a covered entity not having appropriate legal paperwork - “intentional misconduct” bearing a penalty of at least $50,000 and up to $1,500,000
- Not clear if government will audit contract with business associates in new future

3.3. Risks to covered entity associated with “border” provider originated risks

- Any provider any DHS/CC service is affected by border provider’s activity
- Existing but completely absent in risk assessment and risk management – “border risks”
- Caused by system level personnel access to PI data locations and logs – possible altering of both
- Typical services: infrastructure components (firewalls, routers, etc.), security services (web filtering, anti-malware, etc.), application level access (to files or databases, etc.)
- Resolution – separation of duties and physical separation of logging
- All risks (internal risk, service provider internal risk, and covered entity's external risk coming from the service provider) should be outlined in security assurance documents

3.4. Yet one more HIPAA standard – audit trail logs and data retention

- Both PI data owner and service provider's personnel require system/administrative level of access to data
- Possibility of altering of both data and data logs by provider's personnel
- Resolution – separation of duties and saving audit logs on physically separated resource

3.4.1. HIPAA Security Rule Part 164.316 – policies, procedures and documentation requirements

Fundamental HIPAA requirements:

- *"A covered entity must, in accordance with 164.306:*
- *(b)(1) Standard: Documentation.*
- *(ii) If an action, activity, or assessment is required by this sub-part to be documented, maintain a written (which may be electronic) record of the action, activity or assessment.*
- *(2) Implementation specifications:*
- *(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect , whichever is later.*
- *(ii) Availability (required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains."*

3.4.2. Anatomy of Part 164.316 and what it means for service providers (1)

- Maintain a document (a log) of all activities associated with EPHI
- Maintain logs for at least 6 years
- Covered entity is responsible for keeping logs, not a business associate

Some details:

- Logs should be created in the resource associated with EPHI activities, and then stored outside of it
- Logs should be created by each service provider and sent outside of the service infrastructure and saved by covered entity for 6 years
- Logs also should be available for monitoring by cloud and customer personnel.

3.4.2. Anatomy of Part 164.316 and what it means for service providers (2)

- HIPAA does not require service providers to keep logs for 6 years
- However, HITECH considers both covered entities and business associates equally responsible for safeguarding EPHI
- Thus, best practice for providers would be keeping EPHI activity logs for 6 years as well
- It would be helpful as well in a case of a litigation process.

3.4.2. Anatomy of Part 164.316 and what it means for service providers (3)

Requiring a covered entity to keep logs means:

- That such entity must employ an onsite Security Information Management system (SIM) for operations with logs
- Make them available for government audit upon request
- Typical cost is well over $20,000 to purchase plus additional supporting expenses
- Likely being over a budget of an SMB entity

3.5. Conclusion (1)

- Our concept of Delegation of Trust clearly explains legal relationship between covered entity/customer and business associate/service provider and along a chain of sub-contractors/service providers
- Appropriate legal relationship between a covered entity and a cloud require security level agreements between a customer and each of the providers if providers are independent business entities. The number of such agreements is multiplied by the number of customers.
- Implementation of trust requires appropriate security level assurance document which accompany security level agreement. The number of such documents is the same as above, and is equal to the number of providers multiplied by the number of customers.
- If a cloud forms new legal entity, then it should be one cloud-wide security level agreement between all providers and similar - security assurance document. Then each customer should be given two documents representing agreement between the customer and cloud as well as security guarantees.

3.5. Conclusion (2)

- In any case, customer should know all legal entities included in the cloud.
- Legal document of security assurance should include risk assessment and risk management of, as we named them, “border risks”.
- What is said in pp.2 – 7 of this Conclusion, creates enormous legal challenge to DHS/CC providers. Our opinion is that nothing has been done yet by the providers toward making DHS/CC operations truly legal.
- Implementation of HIPAA provisions of keeping documents/logs of all activities concerning EPHI on customer legal premises for 6 years creates a legal and technical challenge for both covered entities and business associates, and in particular considering moving EPHI freely between sub-contractors.
- The requirement of keeping a SIM system to collect logs for 6 years on covered entity’s premises places a high technical and financial burden for SMB size covered entities

4. Final conclusion (1)

In our already technology-overloaded world, any new technology should be carefully investigated to understand its role, capabilities, as well as possible risks. Cloud Computing has been pushed to market and promoted as optimizing IT services. Its current technological capabilities are adequate to address its main purpose. However, legal grounds for this technology have not been investigated prior to moving it forward and promoting to regulated industries. Instead, the research focused more on “operational” aspects of security, not legality of services. Regulations like HIPAA and, more recently, MGL 93H – 201 CMR 17.00 Standards require certain assurance of protection of personal information, and thus establish a legal relationship between providers and customers. When we come to analyze CC from purely legal grounds, we see enormous problems starting with questionable models, unsound architecture, and ending with a necessity of having numerous legal binding instruments, completely uninvestigated risks, and finally deploying heavy duty security systems in a cloud and on customer site to maintain legal compliance. In short, regulated industries and US government in particular cannot use cloud services as they are now and will not be able to use them until a legal ground for the technology is laid down.

4. Final conclusion (2)

Dear Colleagues,

- We hope that our research will stimulate careful consideration of all security problems surrounding “Cloud Computing”. Moreover, we suggest renaming the term itself to a more appropriate “Dynamic Hosting Service” without confusing models. This will help to avoid misleading marketing-oriented terminology and bring the legal aspects of information security to the forefront.
- Thank you very much for participating in this discussion!

References:

1. Shankar B. Chebrolu, PhD, CISSP, et al. Top Ten Risks With Cloud That Will Keep You Awake at Night. OWASP, September 22, 2011.

2. Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, December 2011.

3. DRAFT Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146, May 2011.

4. Department of Health and Human Services/Centers for Medicare and Medicaid Services/ Office of E-Health Standards and Serrvices. Sample – Interview and Document Request for HIPAA Security Onsite Investigation and Compliance Review.

5. Ryan K.L. Ko et al. TrustCloud: A Framework for Accountability and Trust in Cloud Computing, HP Laboratories, IEEEICFP 2011.

Thank you!

All questions will be answered:

- mikhailutin@hotmail.com

or

- mutin@rubos.com

Rubos, Inc. (presentations, texts, articles, etc.)

- www.201cmr17.00ma.com