



## ***Insights into Health Insurance Portability Accountability Act (H.I.P.A.A) and Your Datacenter Move***

### ***Introduction***

Let's start this discussion with two questions. First did you think the Health Insurance Portability Accountability Act was abbreviated H.I.P.A.A.? Second did you think, like most, the P stood for Privacy? Or are you one of the few that knew that Portability was in the title? Now consider that while your servers (containing **Health** information) are in transit (being **ported**) between two datacenters you're **Accountable**.

We believe the H.I.P.A.A regulations apply to in-transit as well as to operational datacenters. Of course we could be wrong; it is entirely possible that the jury will consider any information theft as your carrier's problem. Not being a lawyer, a judge, or a politician we will refrain from even assuming to tell you what to do. We simply ask you: Do you want your business to be the test case?

For the purposes of this paper, we assume you are accountable for the health information privacy while your datacenter is in-transit. It then follows that these sections (excerpts from the Federal Register 45 § 164) are just as applicable to your equipment while it is in the datacenter behind keycard and 24x7 monitoring as it is while it is in the back of a truck.

From the H.I.P.A.A. introduction in the Federal Register:

"Section 1173(d)(2) of the Act states: Each person ... who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards."

This paper addresses what controls you should take to comply with H.I.P.A.A. in the context of moving or consolidating your datacenters.

### ***Federal Register 45 § 164.308 Administrative Safeguards:***

***Subsection (a)(1)(ii)(A) Risk analysis.*** Conduct 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.

Not all moves are equal. A move across town with an hour of exposure does not warrant the same level of detail as a move across the country with days of exposure. The questions to answer are: Has your move team accurately assessed the risks and vulnerabilities to

the protected health information on the machines being moved? Has that risk been communicated to the appropriate personnel in the company to make the right call as to how the move should be handled?

**Subsection (a)(1)(ii)(B) Risk management.** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a)

Once you understand the risks associated with your specific move, what are the specific steps you are taking to reduce those risks? In a simple case, your sysadmin is driving the servers across town in the back of the car. What is the risk here? The sysadmin can do anything to the server while in the datacenter anyway. Your sysadmin may not want to be suspect if an information breach should occur and I expect you want full logging of any server access, which is only available in the datacenter environment. This brings us to the next point.

**Subsection (a)(1)(ii)(D) Information system activity review.** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

It is relatively easy to create and review system activity logs when the servers are in the datacenter. How will you know if the equipment has been accessed, either authorized or unauthorized [see 164.306(a)(1)] while in transit? Who is responsible for creating and reviewing the security incident tracking reports for your equipment while in transit?

**Subsection (a)(6)(i) Standard: Security incident procedures.** Implement policies and procedures to address security incidents. (ii) Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

The best security incident response plans are useless if you do not know a breach has occurred. It is good planning to let the Security Incident Response team know which equipment and what information is being moved prior to the move. So if something should happen the team can quickly respond.

**Subsection (8)(b)(1) Standard: Business associate contracts and other arrangements.** 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's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

This is a very interesting H.I.P.A.A requirement. Do those you trust to move your equipment while in transit between floors, between buildings, or between states have policies and procedures in place to safeguard your information? Have these safeguards been tested? Specifically what is the contractor's plan to track equipment through

the move process and assure that it arrives untampered? How will your carrier demonstrate that nothing happened to the equipment while in their control?

Alcyone Consulting has developed a set of process and procedures to take your team through a risk analysis framework. It is designed to help you make the appropriate business decision regarding the level of security your physical move requires. Once you know the risks associated with the move, we work closely with project management, the equipment carrier and receiving entity to provide the required controls for HIPAA reporting and assurances.

### ***Federal Register 45 § 164.310 Physical Safeguards:***

***Subsection (a)(1) Standard: Facility access controls.*** Implement policies and procedures to limit physical access to ... the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

How do you know, and limit, access to the equipment while it is in transit? The time in transit could be a very short, an hour across town; or very long, a week across the country. Either way it is important to know that the equipment will not experience unauthorized access while in route, and yet on the other end the equipment will be easily accessible.

***Subsection (ii) Facility security plan*** (Addressable). Implement policies procedures to safeguard the facility the equipment therein from unauthorized physical access, tampering, and theft.

There are means to safeguard your equipment while it is in transit between datacenters. A simple means is to seal all the doors to the truck trailer and lock them. There are key questions to address regarding the procedures for that activity:

How do you independently verify the trailer seals at the receiving end? How many keys are available for the locks and who has them? Does the driver have the keys to the truck?trailer? What is your process if the seals are broken? How will you determine which, if any machine was accessed in route?

Other questions to ponder:

What are your procedures to unload and receive the equipment at the destination? Where will the equipment be staged? In an open receiving dock for three hours, waiting for someone to move it into the datacenter? Secure storage facilities? How will the final installer verify the equipment has not been tampered with?

**Subsection (iii) Access control and validation procedures** (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor access.

Who is authorized to sign for the equipment when it arrives? If the equipment is going to a hosting service provider will this be the person who signs for everything or is there someone who is familiar with the sensitivity of the information that is responsible for seeing it through to its destination?

**Subsection (d)(1) Standard: Device and media controls.** Implement policies and procedures that govern the receipt and removal of hardware ... into and out of a facility, and the movement of these items within the facility.

How does this relate to equipment in transit? First ask yourself is the equipment being shipped point-to-point in a secured truck or will the equipment flow through a chain-of-custody? If it is being transported through a chain-of-custody how are you going to verify and communicate the state of the equipment at each hand-off?

**Subsection (iii) Accountability** (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Most common carriers today have an electronic tracking system which will allow you to know the location of your package down to the truck. Do you have an equivalent process in place so you know where your equipment is as it goes through the stages of being un-racked, packed, shipped, received, unpacked, staged, and re-racked? Do you know who is accountable for the equipment at each stage? Do they know how to verify the equipment has not been accessed? Do they know who to contact to confirm receipt of the equipment?

When you use Alcyone's customized sealing technology, you can quickly identify if any machines have been compromised. This allows you to immediately escalate concerns while enroute to your Security Information Response team. Furthermore, you will have a record of accountability for your equipment at each stage, through the chain-of-custody, from the originating datacenter to the destination datacenter. Our services are designed so you can meet the H.I.P.A.A. physical and administrative safeguards.

## **Conclusion**

H.I.P.A.A requires you to have procedures in place which provide reasonable assurance that your equipment with Health related information is safe from unauthorized access and tampering. H.I.P.A.A. also requires you to provide reasonable administrative safeguards so you know when access has occurred and can determine if it is authorized or not.

When moving a datacenter your equipment is not exempt from these precautions. Alcyone has a process that gives you the records you need to show that your equipment has arrived without unauthorized physical access, without tampering, and most importantly your information has remained safe and secure.

## ***About Alcyone Consulting***

Alcyone Consulting is an IT Consultancy providing IT Strategy and Governance services. Our principals have worked together for over a decade providing high quality IT solutions to a wide range of clients. Our practitioners are all former Big-5 consulting professionals with years of experience.

The Alcyone Secure Datacenter Move Service offering is a natural outgrowth of our primary expertise, datacenter and infrastructure management, and our HIPAA and SOX compliance practice with ITIL and CobiT.

At Alcyone Consulting we understand that the IT Service services the Business. We incorporate this into all we do.

***For more information contact Tom Weber:***

***1.773.203.1738  
tweber@alcyonegroup.com***