The Global Impact of the New HIPAA Rules on Cloud Service Providers: A Hypothetical Conversation

TODD TABOR
Senior Counsel, Hewlett-Packard Company, USA

Synopsis
As in house counsel, we are often tasked with wearing multiple hats, not all of which are legal. This can occasionally be a challenge, but in most cases, it represents one of the most exciting aspects of working in house. One such scenario may be on your radar screen now with the updated HIPAA rules issued on January 25, 2013 (FR, Vol 78, No. 17). The new rules have, in many respects, clarified the responsibilities of Covered Entities and Business Associates, but at the same time the new rules have potentially scoped in cloud service providers that may have been operating in a grey area previously. This leaves in house counsel with the responsibility of not only explaining the legal impact of the new rules, but also, in many cases, helping the business make decisions on how the business should be structured moving forward. This paper will dive into some of the details of the newly released rules and how they impact cloud service providers by walking through a hypothetical conversation between a business representative and their in house counsel. As always, this paper is not intended to represent legal advice and should not be taken as such. With that background, we can join the conversation already in progress.

We need to determine if we are subject to what? Did you say HIPAA or hippo?
That was HIPAA. Here is a little background. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress granting the Department of Health and Human Services (HHS) the power to create and enforce rules regarding the protection of Protected Health Information (PHI) and contains the key provisions of what is commonly referred to as the Privacy Rule. You may recognize some of the impacts in your daily life when you have to sign privacy notices at the doctor’s office or when you see certain physical safeguards at your pharmacy that limit who can see what prescriptions you are picking up.

In 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act added clauses around the meaningful use of information technology tools and the privacy and security requirements associated therewith and contains the key provisions of what is commonly referred to as the Security Rule. In short, it covers the electronic versions of your PHI and describes the security tools required (or recommended) to help protect that electronic PHI.

On January 25, 2013, HHS issued a much anticipated set of final rules that became effective March 26, 2013. These final rules substantively impact the Security Rule, and to a lesser extent the Privacy Rule as it relates to Business Associates. In most respects, Covered Entities and Business Associates will need to be compliant with the final rules after September 23, 2013.
I thought HIPAA only applied to hospitals and doctors. Who is covered?
Though there are some nuances, it can be definitively stated that Covered Entities are the primary regulated entities under HIPAA. Without a Covered Entity involved, HIPAA will not apply. By statute, a Covered Entity means an entity that operates as (1) a health plan, (2) a health care clearinghouse, or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

But I am not a Covered Entity; so, why should I care about HIPAA?
Like I said, a Covered Entity must be involved for HIPAA to apply. At some point, I am sure that you will want to do business with a Covered Entity. When you do, you will need to determine if you are acting as a Business Associate. If you are a Business Associate, then certain requirements from HIPAA will flow down to you. This is where the new rules have their first significant impact. The definition of a Business Associate was expanded to include any entity that “provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.” (45 CFR 160.103(3)(i)).

But I do not “require access on a routine basis”. Why am I considered a Business Associate?
Though there is an exclusion for “mere conduits” -- entities like the U.S. Postal Service or internet service providers -- HHS has made it very clear in the comments to the rule that “such a determination will be fact specific” and that the conduit exception “is a narrow one and is intended to exclude only those entities providing mere courier services…and their electronic equivalents”. (FR Vol. 78, No. 17, pg. 5571).

Ok, I agree that my Cloud Services are more than just “courier services”, but we do not need to actually view the electronic PHI. I have heard that if we only have occasional random access to PHI, then we will not be a Business Associate. Is that true?
This exception is part of the conduit rule and perhaps could have been argued previously. However, as part of the new rule, HHS has included in the definition of Business Associate any entity that “maintains” PHI. If the Cloud Services requires the persistent flow of PHI through your systems, you will likely be considered to be a Business Associate, even if you do not view the information. For example, if your services include electronic data storage, then you will need to comply with HIPAA.

But I do not know what is stored on my systems. It is all encrypted, and our employees never look at the information itself.
While that is great news from a compliance perspective, it does not impact the initial analysis. If your cloud services “maintain” the information, even if you never look at that information, you may still be considered a Business Associate.

Maybe a more traditional example will help explain the logic better. Assume that a hospital sends hard copy records to a company that stores those records for a set period of time and then ultimately destroys them after a retention period has past. As part of their service, even though they may have some incidental contact with the actual record, they never actually have to view the records in order to perform the services. HHS has made it very clear that this type of activity would cause a company to be a Business Associate (FR Vol. 78, No.17, Pg. 5573).

Clearly, translating that example into the electronic equivalents could cause any Cloud Service Provider that is providing data storage or backup services for electronic PHI as part of their overall service offering to be considered a Business Associate. Furthermore,
even if you are not providing those specific services as part of your solution, if the electronic PHI will be flowing through your systems, we will have to take a deeper dive to determine if the conduit exception that I talked about previously applies. In either case, if it is reasonable to assume that electronic PHI will be included in the data that is transmitted to you, even if you never view that data, you will likely need to comply with HIPAA.

But I have not had to sign a Business Associate Agreement in the past. If the Covered Entity does not require me to sign one, do I still need to comply with HIPAA?
The Covered Entity has an obligation to put a Business Associate Agreement in place prior to sharing the PHI with another party, subject to a few exceptions. Their failure to do so can impact their liability. However, failure to put one in place does not eliminate the Business Associate’s requirements to comply with HIPAA. If you know or should have known that you were receiving electronic PHI, then you will need to comply with HIPAA.

We are not even sure if we will be providing services from the United States. Can we provide the services from Europe? If so, does that eliminate our compliance obligations?
You can absolutely provide services from outside of the United States. HIPAA does not limit the locations from where services can be provided. However, moving the electronic PHI outside of the United States does not alleviate the HIPAA obligations. If a foreign entity is providing cloud services to a Covered Entity and they are determined to be a Business Associate, then they will need to comply with HIPAA. You can also expect Covered Entities to push for U.S. law to apply in those situations, or at least ensure compliance with U.S. regulatory requirements.

I understand in the past that a Business Associate only had contractual risk associated with a failure to comply. Has that changed?
That is partially true. In the past, the liability was primarily covered by contractual risk tied to the Business Associate Agreement. HHS had very limited recourse against the Business Associate, and if an obligation was not captured in the Business Associate Agreement, then the risk primarily fell to the Covered Entity for non-compliance.

Today, the new rules make it very clear that the Business Associate can be held directly liable for fines and penalties under HIPAA. This applies regardless of whether a Business Associate Agreement is in place and applies even if the Business Associate Agreement fails to include required provisions. As a result, you will have both contractual risk and regulatory compliance risk.

Ok, I understand; so, what do I do now?
We need to review all five of the cloud service offerings that you provide and for each one, analyze the information flow. The first step is to look at all of the potential types of information that will come in; what type of information is it; and does it qualify as electronic PHI.

Our first cloud service offering does not bring in any data at all, and we do not look at data on the Covered Entity’s systems; however, it is marketed to Covered Entities. Do we need to be HIPAA compliant and sign a Business Associate Agreement for this service?
No. The gating question will always be whether you will have electronic PHI on your systems or whether your employees will otherwise be viewing or have access to PHI. Since this service is provided remotely and no electronic PHI will be viewed or
transmitted, this service will not need to be HIPAA compliant and we should not be signing Business Associate Agreements.

Our second cloud service offering does not need to bring in any electronic PHI, but it does require the transfer of data that may have PHI integrated with it. Our existing Covered Entities scrub the information prior to sending it over to us. However, a few Covered Entities have pushed back on doing this work. Does this cloud service need to be HIPAA compliant, and do we need to sign a Business Associate Agreement?

In a strict sense, the cloud service offering does not need to be HIPAA compliant as long as we are not receiving the electronic PHI. The Covered Entity has a legal obligation to provide us only with the minimum necessary amount of PHI that would be needed in order for us to provide the cloud services. The fact that other Covered Entities are able to remove the electronic PHI is strong evidence that we do not need the electronic PHI to provide the cloud services. However, the “minimum necessary” analysis is extremely fact specific and is subject to a reasonableness standard. To truly answer this question, we would need to analyze whether Covered Entities could reasonably eliminate electronic PHI before sending the data to us. If there are scenarios where it is not reasonable, then, if we want to sell to these Covered Entities, we will need to make the cloud service HIPAA compliant and sign a Business Associate Agreement.

As part of our third cloud service offering we will be able to remotely view PHI that is on a Covered Entity’s systems, but electronic PHI will not be transmitted or stored on our systems as part of the cloud service. Do we need to be HIPAA compliant and sign a Business Associate Agreement for this service?

Yes, but not all provisions will apply. Since you will not be handling electronic PHI on your systems as part of the service, the Security Rule will not apply. However, since you will have the potential to view PHI during the course of providing the services, you will need to comply with the Privacy Rule. Therefore, you will need to implement the processes necessary to comply with the Privacy Rule, and a modified version of the Business Associate Agreement covering the Privacy Rule obligations is appropriate.

Our fourth cloud service offering receives and stores information. We do not know what the information is, but we think it is reasonable to assume that it will include electronic PHI when used by a Covered Entity. Based on our previous discussion, I assume that we will need to make this service HIPAA compliant with both the Privacy and Security Rule. Am I correct?

Now you are catching on. Even though you do not know what is flowing through your systems, since it is reasonable to assume that electronic PHI will be included, the cloud services will need to be compliant with the Security Rule and the Privacy Rule and you will need to execute a full Business Associate Agreement.

Our fifth cloud service offering receives and stores electronic PHI and has been operating for the past few years. We are already compliant with our requirements in our Business Associate Agreements. Is there anything else that we need to do?

Yes. There are two key areas that need to be addressed for the existing cloud service offering. First, the security requirements were modified such that the Business Associate must now comply with specific sections of the Security Rule. Though it is likely that you already comply, a risk assessment and gap analysis will need to be completed to ensure full compliance. Second, certain provisions of the Business Associate Agreement will need to be amended. HHS has given us some extra time to complete this step. All existing Business Associate Agreements must be updated by September 22, 2014 unless renewed
or amended earlier, in which case it must be updated at the time of such renewal or amendment.

**For the cloud services where we will be a Business Associate, what do we need to do to comply with the Security Rule and the Privacy Rule?**

We pick back up the information flow analysis. Once the information is on your system, who has access to it (both actual and potential)? How does it move and where does it go? A risk assessment should be conducted to help answer these questions and determine any gaps between what is required and what is currently implemented. You can then begin to implement steps to mitigate the gaps identified. With that said, you mentioned earlier that the electronic PHI is encrypted at all times while on our systems. This goes a long way towards compliance and is an excellent first step.

**We have talked about inflow and where the electronic PHI moves and resides; so, I guess the next step is outflow. Is that right?**

Exactly. But outflow can take on several different characteristics; so, let me break it down into general categories. The first is outflow to subcontractors. If you have a need to send electronic PHI to a subcontractor, you will need to make sure that the subcontractor also signs an agreement (we will call it a Subcontractor Agreement) binding them to similar (or more restrictive) terms than what you agreed to with the Covered Entity. You will also want to make sure you flow down the same obligation to their subcontractors, if applicable.

**Does the Covered Entity need to sign or review my Subcontractor Agreement with my subcontractor?**

No. The Covered Entity only needs to have privity of contract with their Business Associate. The Business Associate is responsible for entering into a Subcontractor Agreement with their subcontractor, if appropriate.

**If I have a cloud service that needs to be HIPAA compliant, and I am using a subcontractor to provide a piece of the cloud service where they will have no access to, and not receive any, electronic PHI, do I still need to enter into a Subcontractor Agreement with them?**

No. The same gating question applies to subcontractors. If they do not receive or have access to PHI of any kind, then they are not a Business Associate.

**I think I got us sidetracked with the subcontractor questions, what are the other forms of outflow?**

Those were all good questions; so, feel free to continue to interrupt as needed. With that said, the next form of outflow is to the Covered Entity/Individual. In most cases, for the cloud services you are providing you will only be sending information to the Covered Entity; so, I will focus on that piece. However, I wanted to make you aware, that for certain cloud services, you may also have to provide information to the Individual whose information you are handling.

For electronic PHI flowing to the Covered Entity, you will need to determine if the flow is a permanent transfer or temporary. If a permanent transfer, then your Security Rule obligations related to that electronic PHI will end with that transfer, and you will just need a process to track the electronic PHI up and until transfer. If a temporary transfer, then you will need to continue to track the flow of the electronic PHI for as long as it is in your systems.

The final type of outflow is destruction. There are many different techniques for destroying information, and it should only be destroyed in compliance with the agreement with the Covered Entity and applicable law. Typically, the Covered Entity will
have retention requirements for certain PHI and will pass those onto you if they are applicable to the cloud services being provided. Without getting into too much detail related to the process of destroying the electronic PHI, once properly destroyed, your Security Rule obligations related to that electronic PHI will cease.

**Well that seems easy enough. Anything else related to destruction?**
Yes. You also need to consider destruction of electronic PHI that is in a device that is no longer working. When running a cloud service, you will inevitably have a piece of hardware or media fail. In those scenarios, you will need to ensure that you have a process to destroy the electronic PHI that may still be resident on the hardware or media. Once again, there are many ways to accomplish this; so, I will not delve into the details of destruction.

**So, what is next?**
We have determined which of your cloud services are impacted by the new HIPAA rules and have dug deeper into the information flow for those services and discussed completing risk assessments and implementing strategies to obtain compliance to the Security Rule where applicable. The next step will be to create the processes, procedures, and training necessary to comply with the Privacy Rule. In short, we need to make sure that our teams are only receiving, accessing, using, and disclosing the minimum amount of PHI that is reasonably necessary for them to provide the cloud services.

**Ok. Thanks for all of your help. It looks like we will be working quite a bit together over the next couple of months.**
I look forward to it.

**Conclusion**
The job on in house counsel can be complicated to say the least. However, being able to provide clients with sound legal advice that factors in business realities can be exciting. Helping our clients understand the potential impact of the new HIPAA rules on cloud service providers is just another opportunity to do just that. Though some cloud service providers have clearly been providing cloud services that require them to operate as a Business Associate, others have been operating in a grey area or have otherwise been looped in by the recent changes to the rules. Ultimately, who is and is not a Business Associate has become somewhat clearer, and the legal obligations of Business Associates have become much clearer. As you continue to work with your business colleagues in developing new and exciting cloud services offerings, make sure you keep HIPAA compliance on your checklist of potential legal requirements.

***

**Todd Tabor** is Senior Counsel at Hewlett-Packard Company and joined the company thirteen years ago. During his tenure, Todd has served many roles, including HP’s Global Privacy and Security Lead for the HP Software, Cloud, and Open Source group. Todd is also a member of the International Association of Privacy Professionals.

**Hewlett-Packard Company** is one of the leading Cloud Service Providers in the world and also a Platinum Member of the International Association of Privacy Professionals. HP’s goal is to create new possibilities for technology to have a meaningful impact on people, businesses, governments, and society.