vynamic®

VYNAMIC INSIGHT

# MOVING PHI DATA

EXPERTISE & SERVICES: Healthcare Technology


**AUTHORS**

David Leacy
Nicole Werner
Christopher Savage


## Moving your data is complicated and risky enough, but when you are responsible for moving data classified as Protected Health Information (PHI) the stakes are even greater.

Not only is PHI data governed by Health Insurance Portability and Accountability Act (HIPAA) regulations which need to be carefully considered before, during, and after a move, the ever-growing threat of data breaches should make you think twice about shortchanging the planning process. Unfortunately, data breaches in the Healthcare Industry have continued to increase over the past 10 years.

According to Healthcare IT News, between 2009 and 2014, 42 million people have had their data compromised.[1] In 2015, it was discovered up to 80 million patient and employee records were compromised in one attack on an Anthem computer system.[2] While many of these breaches were the result of hacking into a data center, or theft of personal computers with PHI on them, figures like this underscore the importance of managing potential threats when moving data and assets between data centers.

Between 2009 and 2014,

**42M**

people have had their data compromised.[1]

In 2015,

**80M**

patient and employee records were compromised in one attack on an Anthem computer system.[2]

As the healthcare industry continues to demand greater service and quality from all stakeholders, businesses are moving quickly to respond and maintain a competitive edge, often by expanding their offerings using the latest in connected or hosted technologies. Doing so can expose PHI data to environments outside of your direct control which means you must invest the appropriate time and resources to ensure that you and key internal and external stakeholders view securing your data as their number one priority. As you look to migrate data from a private data center to either a hosted or cloud platform, consider these 5 steps to increase the likelihood of a successful migration.

## 1. ASSEMBLE YOUR TEAM

Moving or integrating PHI data is not just a technology team's responsibility. In addition to having representation from system owners, you will need to involve your Information Security Officer and your Legal department. The Security Officer will help you navigate HIPAA regulations and ensure compliance with internal data security standards and industry best practices. They will also validate the plans you define and will often be required to formally review and approve the methods used to migrate PHI data. Legal representatives are required when contracting with partners who will have access to PHI data. If this applies to your scenario, the appropriate Business Associate Agreements (BAA) for covered entities will need to be established following HIPAA guidelines for PHI data prior to allowing access to your data.

## 2. VET YOUR PARTNERS

Vendors often play a significant role in the data migration process – either as a key driver of the data migration or in managing the data once it has reached its destination. In many cases because you are trusting these vendors with sensitive information, you should ensure they are carefully vetted. In addition to the standard due diligence performed during a vendor assessment to select a partner, the addition of PHI data increases the complexity and time required to complete that assessment. Your Security Officer may require physical audits of partner locations and detailed scrutiny of data management policies and procedures. The right partners will have established processes for handling PHI data during and post move, along with a comprehensive data management program based on both HIPAA and industry security standards.

## 3. PROTECT YOUR DATA

Protecting your data entails not only the technical and physical options you deploy but also the surrounding processes and oversight you put in place to safeguard your specific situation. If moving or migrating your PHI data, here are a few important points to consider.

### Inventory and classification

One of the first steps in planning for a data move is creating a comprehensive view of what you need to move. Whether you are moving physical hardware, applications, or just data, having a complete inventory will form the basis for planning and, ultimately, the execution of your move. If you do not currently have an accurate inventory of your environment, invest the time to create one and be sure to maintain it. Auto discovery tools work well to speed up data collection but be prepared to conduct manual searches to track the complete list down. More importantly, classify each asset, application, and data based on whether it contains PHI or not. While best practices should be applied when moving both PHI and non-PHI assets, those assets containing PHI should receive greater scrutiny and employ the strictest policies during execution. Budget or time constraints may warrant using less strict policies for non-PHI data.

### Encryption and secure transit

Guarding against unauthorized access to your data, especially when in transit, is critical. How will you protect your data as it moves over the wire from source to destination? Network engineering should be consulted to implement data transport security protocols, most commonly SSL (Secure Sockets Layer) or TLS (Transport Layer Security) that will guard against vulnerabilities.

### Physical move logistics

Physically moving assets that contain PHI data is where procedural controls are most effective. You should work with your logistics vendor and other partners to implement a formal chain-of-custody (CoC) process that will document – via paper or electronic forms – the hand-offs and continuous possession between approved parties from source location to destination. The CoC also covers the condition of the equipment ensuring that it is delivered in the same condition it was received. Real-time monitoring of the physical move by your Information Security team, and their inclusion as part of the CoC sign-offs, is also recommended.

### Destruction services

In many cases, performing a move event becomes an opportunity to optimize your environment which could result in excess equipment and hard drives you no longer need. Wiping these drives and recycling is one option, but when PHI is involved, drive destruction services remove any doubt that your data will be compromised. When contracting for these services, ensure the provider will furnish formal certificates of destruction as part of the CoC process. This lack of proper destruction and CoC has caused a black-eye for Visionworks, Inc. which had to issue two notices of potential HIPAA data exposure in 2014 after misplacing two database servers they thought they had destroyed, containing information on about 75,000 and 48,000 patients respectively. [3,4]

## 4. ADJUST YOUR POLICIES AND PROCEDURES

An often forgotten activity of a move event is updating a company's existing policies and standard operating procedures, specifically those that govern data. It is likely that the new steady-state in which your PHI data now resides differs than before. And so data management policies, incident response plans, Business Continuity and Disaster Recovery (BCDR) and business-as-usual processes should be reviewed and updated accordingly.

## 5. PLAN AND EXECUTE YOUR MOVE

Even with the best team and partners assembled and using the most secure practices available, nothing ensures success more than a well-constructed plan. Planning to move or integrate PHI data requires the right balance of project planning and risk management. Balancing customer demands, level of risk, and the usual time, budget, and quality constraints is no easy task. The level of risk that PHI presents makes some of the trade-off discussions that much more difficult.
A successful plan is one that has considered all factors, evaluated multiple options, and proceeds only after all stakeholders are aligned and on board. Additionally, once you move to execution, stick to the plan but ensure you have the requisite security and legal stakeholders available should an unforeseen issue arise throughout the move.

The responsibilities that come with managing PHI data are immense. Financial penalties and impacts to a company's reputation due to mistakes, either intentional or not, are a reminder of what's at stake. Between May, 2013 and June, 2014, the Office for Civil Rights levied more than $10M million in fines against organizations that violated HIPAA rules, and many experts expect that number to rise dramatically.[5] When the need to move PHI data cannot be avoided, understanding how best to mitigate the risks can make all the difference. Remember, moving your data is complicated and risky enough.

**Interested in learning more?**
info@vynamic.com
888-VYNAMIC

**END NOTES:**

[1] McCann, Erin. "The Biggest Data Breaches of 2014." HealthcareITNews. December 26, 2014. Downloaded April 8, 2015: http://www.healthcareitnews.com/slideshow/biggest-hipaa-breaches-2014

[2] Kern, Christine. "Anthem Breach Continues to Cause Waves." HealthITOutcomes. February 23, 2015. Downloaded April 9, 2015: http://www.healthitoutcomes.com/doc/anthem-data-breach-continues-cause-waves-0001

[3,4] Visionworks. "Statement on Recent Visionworks Privacy Issue." November 10, 2014. Downloaded April 23, 2015: http://www.visionworks.com/announcement/

[5] Mullaney, Tim. "Recent record-breaking HIPAA fines will be 'low' compared to what's coming, government attorney says." June 17, 2014. Downloaded April 23, 2015: http://www.mcknights.com/news/recent-record-breaking-hipaa-fines-will-be-low-compared-to-whats-coming-government-attorney-says/article/356006/